QEmu – Emulateur rapide

Mode d'emploi pour un hôte Windows

Copyright (c) 2006, Denis SCHEIDT.

Le contenu de ce document peut être redistribué sous les conditions énoncées dans la Licence pour Documents Libres version 1.1 ou ultérieure.

Le document original est consultable sur http://denis.scheidt.free.fr

Le texte complet de la licence peut être consulté à l'adresse :
http://guilde.jeunes-chercheurs.org/Guilde/Licence/ldl.html

Table des matières

1 Avant-propos 4
2 Présentation de QEmu 4
2.1 Qu'est-ce que QEmu ? 4
2.2 A quoi ça sert ? 5
3 Installer QEmu 5
3.1 Télécharger une version précompilée 6
3.2 Compiler à partir des sources 6
3.2.1 Préparation de l'environnement de compilation 6
3.2.1.1 Téléchargement des outils nécessaires 6
3.2.1.2 Construction de l'environnement 7
3.2.2 Télécharger le code source 8
3.2.3 Appliquer un patch 8
3.2.4 Compilation des sources 9
3.2.5 Installation 10
3.3 Module accélérateur 11
3.3.1 Télécharger Kqemu 11
3.3.2 Installer Kqemu 12
4 Démarrage rapide de QEmu 12
4.1 Les périphériques de stockage 14
4.1.1 Créer un disque dur virtuel 14
4.1.2 Les périphériques physiques 14
4.2 Installation d'un système d'exploitation dans QEmu 14
4.2.1 Processeur hôte à coeurs multiples 15
4.2.2 Télécharger des images pré-installées 15
4.2.3 Installer soi-même son système 16
4.2.4 Remarques 17
4.2.4.1 Capture de la souris 17
4.2.4.2 Utilisation élevée du processeur 18
4.2.5 Interfaces graphiques 18
4.3 Installer des applications dans le SE cible 18
5 Utilisation avancée 19
5.1 Images disques – options avancées 19
5.1.1 Les différents formats d'images 20
5.1.1.1 Le format raw 20
5.1.1.2 Le format qcow2 20
5.1.1.3 Les autres formats 20
5.1.2 Les images de base 21
5.1.3 Autres commandes 21
5.2 La ligne de commande 22
5.2.1 Support réseau 22
5.2.1.1 Architecture réseau de QEmu 22
5.2.1.1.1 Mode utilisateur 23
5.2.1.1.2 Mode TUN/TAP 24
5.2.1.2 VLAN 24
5.2.1.3 Autres options réseau 25
5.2.2 Partage de fichiers avec l'hôte 25
5.2.2.1 La disquette 25

5.2.2.2 Partage Microsoft 25
5.2.2.3 Partage de répertoire hôte 26
5.2.2.4 Partage par TFTP 27
5.2.2.5 Partage par SMB 27
5.2.3 Support USB 27
5.2.4 Support Audio 27
5.2.5 Support VNC 29
5.2.6 Autres options 29
5.3 Le moniteur 30
5.3.1 La commande info 31
5.3.2 Éjecter/Changer un CD ou une disquette 32
5.3.3 Redémarrer la machine virtuelle 32
5.3.4 Suspendre/Éteindre QEmu 32
5.3.5 Commandes USB 32
5.3.6 Envoyer des séquences de touches 33
5.3.7 Sauver/Charger la machine virtuelle 33
5.3.8 Autres commandes 34
6 Utilitaires divers 34
7 Liens 35
8 Copies d'écrans 36
9 Annexes 38
9.1 Liste des codes sendkey 38
10 A faire 39
11 Historique des modifications 40
1 Introduction 41
2 Définitions et domaine d'application 41
3 Conditions communes aux versions modifiées et intégrales 41
4 Modifications 42
4.1 Dispositions générales 42
4.2 Fusion ou combinaisons de documents 42
4.3 Inclusion dans d'autres travaux 42
4.4 Traduction 42
5 Dispositions concernant la garantie 42
6 Cessation de la licence 42
7 Évolution de la licence 42

1 Avant-propos

L'émulateur QEmu peut être utilisé sur bon nombre de plates-formes, et peut émuler plusieurs systèmes différents.

Ce manuel se limite à l'installation et à la configuration de la version de QEmu pour Windows, dans le cadre de l'émulation d'un système x86. Les autres plate-formes hôte et cible ne sont pas abordées ici.

De même, ce document ne couvre pas l'installation complète d'un Système d'exploitation dans la machine virtuelle, chaque système ayant sa propre procédure, mais se borne à donner les conseils nécessaires à *l'assemblage des composants* et à la bonne utilisation du *matériel virtuel* proposé par QEmu.

Ce manuel représente la somme de mon expérience personnelle de QEmu et des différentes informations trouvées sur les forums dédiés et la liste de diffusion des développeurs.

Définitions :

- le terme **hôte** s'applique au système sur lequel le fichier **qemu.exe** est exécuté. Dans le cadre défini pour ce manuel, ce sera un PC x86 (à base de processeur Intel ou AMD), tournant sous Windows (quelle que soit la version, mais Windows 2000 ou supérieur est fortement recommandé, dans la mesure où ces systèmes sont plus stables et plus efficaces que les versions 9x).
- Les termes **cible**, **machine virtuelle** s'appliquent au système émulé, celui qui « tourne à l'intérieur de la fenêtre ». Le manuel se limite à l'émulation d'un système x86. Mais rien ne vous empêche ensuite d'explorer les autres architectures.
- Le terme **virtuel** s'applique au système émulé, par opposition aux termes **réel** et **physique** qui concernent le système hôte.
- l'abréviation **SE** est utilisée pour « Système d'exploitation ».

Pour vos explorations du monde QEmu, prévoyez tout de même une configuration relativement musclée. L'émulation a besoin d'un processeur rapide et de beaucoup de mémoire pour atteindre des vitesses acceptables. Pour donner un ordre de grandeur, 512 Mo de RAM et un processeur à 1 GHz semblent le minimum pour envisager une utilisation sérieuse de la machine virtuelle. Cette limite peut varier en fonction du SE cible installé dans la machine virtuelle : MS-DOS, Linux en mode texte, par exemple, peuvent être utilisables sur une configuration nettement moins puissante.

QEmu est actuellement assez instable sur les processeurs à plusieurs coeurs, ainsi que les Pentium HyperThreading. Voyez le paragraphe 4.2.1, page 15.

QEmu étant en évolution permanente, certaines fonctionnalités décrites peuvent (vont) évoluer. Ce guide sera mis à jour le plus régulièrement possible pour refléter au mieux les changements de QEmu.

Si vous constatez une incohérence, une erreur ou une imprécision, ou si une option semble ne pas fonctionner conformément à la description faite dans ce guide, ou juste pour me dire que ce guide vous a été utile, envoyez-moi un mail à l'adresse suivante : qemuwindoc@free.fr

2 Présentation de QEmu

2.1 Qu'est-ce que QEmu ?

QEmu (http://fr.wikipedia.org/wiki/Qemu) est un émulateur, c'est-à-dire un **logiciel** qui reproduit le fonctionnement d'un **matériel** (http://fr.wikipedia.org/wiki/Emulateur).

QEmu n'émule pas simplement le processeur, mais un **ordinateur complet**, du clavier à la carte graphique, en passant par les disques et la carte réseau.

Dans le cas de l'émulation PC, QEmu embarque le matériel suivant (pour les connaisseurs ☺):

- processeur Pentium II
- chipset i440FX
- pont PCI vers ISA PIIX3
- carte graphique PCI Cirrus CLGD 5446
- souris et clavier PS/2
- 2 contrôleurs IDE PCI, supportant des disques durs et lecteurs de CD/DVD

- 1 contrôleur de disquettes
- 1 ou plusieurs cartes réseau PCI NE2000
- 1 ou plusieurs ports série
- 1 carte sonore SoundBlaster 16
- 1 carte PCI audio ENSONIQ AudioPCI ES1370
- 1 chip compatible Adlib(OPL2) – Yamaha YM3812
- 1 contrôleur USB UHCI PCI, 1 hub USB

QEmu peut émuler de 1 à 255 processeurs.

Bref, pour simplifier, lorsque vous lancez QEmu, vous retrouvez dans une fenêtre exactement ce que vous avez sur votre bureau : un ordinateur complet, en ordre de marche.

Mais QEmu ne se limite pas à l'architecture Intel. Il peut également émuler des systèmes à base de processeurs x86 64 bits, ARM, SPARC, SPARC 64, PowerPC, MIPS, m68k et SH-4. De plus, il peut être compilé et utilisé sur la plupart de ces systèmes.

La liste complète des systèmes émulés est disponible sur le site de l'auteur (http://qemu.org/status.html).

En règle générale, un émulateur est nettement plus lent que le système réel sur lequel il s'exécute. C'est normal, puisque chaque instruction du système cible doit être interprétée, pour engendrer l'action correspondante sur le système hôte.

QEmu utilise une technique différente, appelée **compilation dynamique**. Le code du système cible est lu par blocs (un bloc étant en général la portion de code contenue entre deux sauts ou branchement), puis traduit en code du système hôte, et enfin compilé au vol avant d'être exécuté par le processeur hôte. Cette technique lui permet d'être plus rapide qu'un système utilisant simplement une interprétation du code cible. De plus amples information, en anglais, ici : http://qemu.org/qemu-tech.html.

Dans le cas d'un système cible x86 sur un hôte x86, il existe un module accélérateur (Kqemu), qui permet d'augmenter encore la vitesse de l'émulateur. Dans ce cas, le code cible n'a pas besoin d'être compilé au vol, et s'exécute directement sur le processeur hôte. QEmu est ici plus proche de la virtualisation (http://fr.wikipedia.org/wiki/Virtualisation) que de l'émulation.

QEmu est l'oeuvre de Fabrice Bellard (http://fabrice.bellard.free.fr).

QEmu est régi par la licence LGPL.

L'accélérateur Kqemu est un module propriétaire, mais son utilisation est libre. Toute redistribution de ce module doit toutefois être soumise à acceptation de l'auteur.

2.2 A quoi ça sert ?

Voilà une question à laquelle il n'est pas forcément facile de répondre, tant cela dépend des centres d'intérêts de chacun.

Quelques unes des raisons, dans le désordre, qui peuvent motiver l'utilisation d'un émulateur tel que QEmu :

- utiliser Linux, ou MacOS, ou d'autres OS, dans un environnement Windows, et pouvoir passer instantanément de l'un à l'autre, sans multi-boot donc sans être obligé de redémarrer le PC ;
- ou bien l'inverse...
- tester des logiciels sans obligatoirement polluer la machine sur laquelle on travaille d'habitude ;
- faciliter le développement et le débogage d'un nouvel OS ;
- faire tourner d'anciens logiciels que Windows XP ne supporte plus ;
- pour un développeur, tester ses propres jeux d'installations sur une machine toujours propre (qui n'a jamais installé son application chez un client pour s'apercevoir que ça ne marche pas, alors que tout semblait OK sur le poste de développement) ;
- etc, etc...

3 Installer QEmu

Pour pouvoir utiliser QEmu, plusieurs solutions se présentent à nous : on peut trouver sur le web des versions déjà compilées, ou alors on peut décider de faire cette compilation soi-même.

La première approche présente l'avantage de la simplicité, mais elle est tributaire de la fréquence de mise à jour et des choix de modules et/ou de patches définis par l'administrateur du site.

Il faut savoir que QEmu, qui en est aujourd'hui (juillet 2006) à sa version 0.8.2, est en évolution constante. Son auteur peut publier des modifications jusqu'à plusieurs fois par semaine.

Pour suivre au plus près ces améliorations, la seconde méthode présente bien plus de souplesse, mais nécessite un peu plus de préparation.

3.1 Télécharger une version précompilée

Plusieurs sites proposent des versions prêtes à l'emploi pour Windows. Cette liste est loin d'être exhaustive.

Attention : certains sites proposent des versions *patchées* (les patches sont des modifications destinées à corriger certains défauts ou apporter des améliorations, mais qui n'ont pas été intégrées dans QEmu par Fabrice BELLARD).

Adresse	*Commentaires*
http://daimon55.free.fr/qemu/qemu.html	Le site de Ronald DELOBEL. Pas de mise à jour depuis novembre 2005. Version non patchée.
http://www.h7.dion.ne.jp/~qemu-win/	Plusieurs versions patchées et expérimentales, et beaucoup d'informations et de liens en tout genre.
http://denis.scheidt.free.fr	Exécutable qemu pour Windows, sans installation.

3.2 Compiler à partir des sources

Le projet QEmu est hébergé sur le site Savannah (http://savannah.nongnu.org), spécialisé dans la fourniture d'outils et de services pour la création de logiciels libres.

QEmu est écrit en C. La partie multimédia met à contribution les bibliothèques SDL. QEmu est optimisé pour être compilé avec GCC 3.x. Utiliser une version plus récente risque de produire un résultat inutilisable.

Le code source de QEmu est accessible au travers du système de gestion de versions CVS (Concurrent Versions System – http://fr.wikipedia.org/wiki/CVS)

3.2.1 Préparation de l'environnement de compilation

QEmu a vu le jour dans un environnement Linux. Afin de pouvoir compiler le projet sous Windows, il nous faut d'abord recréer cet environnement permettant aux outils utilisés de fonctionner correctement.

Si l'anglais ne vous fait pas peur, il existe une procédure toute faite ici : http://qemu.dad-answers.com/viewtopic.php?t=73. Merci à Comike (http://perso.wanadoo.es/comike) pour son mode d'emploi, qui m'a bien servi d'ailleurs pour compiler mes propres versions.

3.2.1.1 Téléchargement des outils nécessaires

Pour pouvoir compiler facilement le code source de QEmu, nous devons lui préparer un environnement aussi proche que possible de son environnement natif. Voici donc la liste des composants à télécharger et à installer.

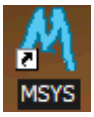
Composant	*Lien*	*Commentaire*
MSYS-1.0.10	http://prdownloads.sf.net/mingw/MSYS-1.0.10.exe?download	Shell Linux pour Windows. Permet de taper des commandes comme si on était sous Linux.
MsysDTK-1.0.1	http://prdownloads.sf.net/mingw/msysDTK-1.0.1.exe?download	Composants supplémentaires pour permettre la compilation de MSYS.
MinGW-3.1	http://prdownloads.sf.net/mingw/MinGW-3.1.0-1.exe?download	Le compilateur GCC proprement dit, dans sa version adaptée pour Windows.
SDL-1.2.8	http://www.libsdl.org/release/SDL-1.2.8.tar.gz	La bibliothèque multimedia utilisée pour QEmu.
Zlib-1.2.2	http://prdownloads.sourceforge.net/libpng/zlib-1.2.2.tar.gz?download	Support des images PNG

Composant	*Lien*	*Commentaire*
Directx-devel	http://www.libsdl.org/extras/win32/common	Support DirectX

3.2.1.2 Construction de l'environnement

- Installez MSYS dans le dossier de votre choix (C:\MSYS par exemple). Si vous voyez un message vous demandant si vous voulez exécuter une post-installation (post install), répondez par N (non).
- Installez msysDTK **dans le même dossier** (C:\MSYS).
- Installez MinGW dans le dossier **mingw** sous **MSYS** (C:\MSYS\MinGW). Si l'installeur affiche un message indiquant que le dossier existe déjà, cliquez sur **Oui** pour confirmer l'utilisation de ce dossier.

L'étape suivante se déroule dans MSYS. Repérez l'icône MSYS que l'installation a du créer sur votre bureau, et double-cliquez la.



Vous vous trouvez maintenant dans un shell de type Linux.

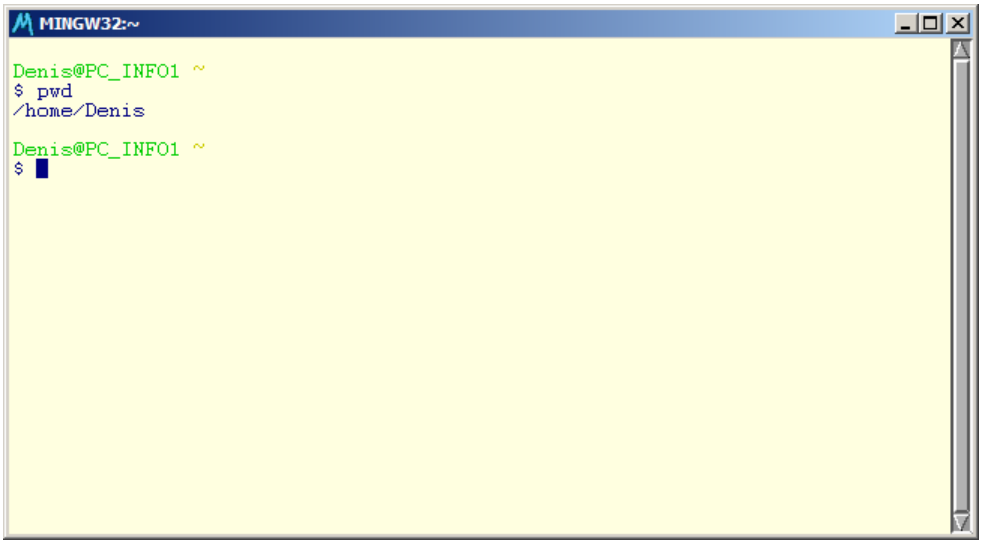


Illustration 1: Environnement MSYS

A l'invite **$**, tapez la commande pwd (ne tapez jamais le $ en début de ligne, c'est l'invite)

```
$ pwd
/home/<NomUtilisateur>
```

La commande affiche alors le nom du dossier courant : /home/<NomUtilisateur>

Avec l'explorateur Windows (par exemple), copiez les fichiers **SDL-1.2.8.tar.gz**, **zlib-1.2.2.tar.gz** et **directx-devel.tar.gz** dans le dossier C:\MSYS\home\<NomUtilisateur>.

Installation de directx-devel :

```
$ cd
$ tar -C /mingw -xzvf directx-devel.tar.gz
```

Compilation et installation de SDL :

```
$ tar -xzvf SDL-1.2.8.tar.gz
$ cd SDL-1.2.8
$ ./configure --prefix=/mingw
$ make
$ make install
```

Compilation et installation de zlib :

```
$ cd
$ tar -xzvf zlib-1.2.2.tar.gz
$ cd zlib-1.2.2
$ ./configure -prefix=/mingw
$ make test
$ make install
```

Ces opérations peuvent prendre quelques minutes, soyez patient...

Maintenant que cette étape est terminée, notre environnement est prêt pour la compilation de QEmu proprement dit. En principe, vous n'aurez pas besoin de repasser par cette préparation.

3.2.2 Télécharger le code source

Cette opération se déroule dans l'environnement MSYS, démarrez-le si ce n'est déjà fait.

Avant de compiler QEmu, il faut télécharger les derniers sources depuis le dépôt CVS. Assurez-vous d'être dans votre dossier racine (/home/<NomUtilisateur>) avant de mettre les sources à jour.

```
$ cd
$ cvs -z3 -d:pserver:anoncvs@cvs.savannah.nongnu.org:/cvsroot/qemu co qemu
```

Cette commande va rapatrier les derniers changements appliqués au code source par l'auteur. Nous sommes maintenant prêts pour lancer la compilation.

3.2.3 Appliquer un patch

Vous trouverez assez facilement des patches pour qemu, car bon nombre de développeurs à travers le monde corrigent et améliorent le programme tous les jours, même si la décision finale d'intégrer telle ou telle portion de code appartient généralement à Fabrice BELLARD. La liste de diffusion des développeurs (http://lists.gnu.org/archive/html/qemu-devel/) est l'endroit idéal pour glaner ces petites modifications.

Si vous désirez appliquer un correctif avant de compiler les sources, voici comment procéder.

Créez tout d'abord un dossier dans lequel vous placerez vos rustines. Je vous propose d'utiliser le répertoire /home/<NomUtilisateur>/patch. Copiez le fichier contenant le correctif dans ce dossier. Les patches se présentent généralement sous la forme d'un fichier diff, comme dans l'exemple suivant :

```
Index: vl.c
===================================================================
RCS file: /sources/qemu/qemu/vl.c,v
retrieving revision 1.206
diff -u -r1.206 vl.c
--- vl.c    6 Aug 2006 13:36:11 -0000     1.206
+++ vl.c    7 Aug 2006 03:53:22 -0000
@@ -4539,7 +4539,11 @@
     BlockDriverInfo bdi1, *bdi = &bdi1;
     QEMUFile *f;
     int saved_vm_running;
+#ifdef _WIN32
+    struct _timeb tb;
+#else
     struct timeval tv;
+#endif

     bs = get_bs_snapshots();
     if (!bs) {
@@ -4567,9 +4571,15 @@
     }
```

```
     /* fill auxiliary fields */
+#ifdef _WIN32
+    _ftime(&tb);
+    sn->date_sec = tb.time;
+    sn->date_nsec = tb.millitm * 1000000;
+#else
     gettimeofday(&tv, NULL);
     sn->date_sec = tv.tv_sec;
     sn->date_nsec = tv.tv_usec * 1000;
+#endif
     sn->vm_clock_nsec = qemu_get_clock(vm_clock);

     if (bdrv_get_info(bs, bdi) < 0 || bdi->vm_state_offset <= 0) {
```

Ce fichier liste les modifications à apporter aux fichiers sources que vous avez téléchargés. L'exemple ci-dessus s'applique à vl.c, mais plusieurs fichiers sources peuvent être modifiés par le même patch.

Placez vous dans le répertoire qemu, puis appliquez le patch avec les instructions suivantes :

```
$ cd qemu
$ patch < ../patch/qemu-20060807-compile.patch
patching file `vl.c'
```

Le nom du fichier contenant le code modifié est ici `qemu-20060807-compile.patch`, mais il est évident qu'il faudra le remplacer par celui du fichier que vous aurez téléchargé.

Vous pouvez maintenant passer au chapitre suivant pour lancer la compilation.

Si le correctif cause l'échec de la compilation, remettez simplement tous vos sources à jour avec la commande cvs.

3.2.4 Compilation des sources

```
$ cd qemu
$ ./configure -target-list=i386-softmmu --static
```

Le résultat de cette commande doit ressembler à ceci :

```
Install prefix    /c/Program Files/Qemu
BIOS directory    /c/Program Files/Qemu
binary directory  /c/Program Files/Qemu
Source path       /home/Denis/qemu
C compiler        gcc
Host C compiler   gcc
make              make
install           install
host CPU          i386
host big endian   no
target list       i386-softmmu
gprof enabled     no
profiler          no
static build      yes
SDL support       yes
SDL static link   yes
mingw32 support   yes
Adlib support     no
CoreAudio support no
ALSA support      no
DSound support    no
FMOD support      no
kqemu support     yes
```

```
Documentation     no
```

Vérifier surtout les lignes SDL. Elles doivent être à « yes ». Si ce n'est pas le cas, retournez à l'étape d'extraction et d'installation de SDL (Construction de l'environnement), puis continuez la procédure jusqu'à arriver ici de nouveau. Si la ligne Documentation est à « no », ce n'est pas un problème.

La compilation, enfin !, se lance par :

```
$ make
```

Quelques messages d'avertissement (Warning) peuvent s'afficher pendant la compilation. Ce n'est pas un problème. A la fin de la compilation, vérifiez qu'il n'y a pas d'erreur.

Si la compilation se termine sur une erreur, entrez une commande make clean, puis relancez make. Si cela ne corrige pas l'erreur, il est possible que l'un des fichiers sources contienne une erreur : attendez alors quelques heures, puis mettez vos sources à jour; les erreurs de ce type sont souvent corrigées très rapidement.

Une dernière étape, facultative, va permettre de réduire un peu la taille de l'exécutable en retirant toutes les informations inutiles.

```
$ strip i386-softmmu/qemu.exe
$ strip qemu-img.exe
```

Nous avons maintenant deux fichiers exécutables :

C:\MSYS\home\<NomUtilisateur>\qemu\i386-softmmu\qemu.exe

C:\MSYS\home\<NomUtilisateur>\qemu\qemu-img.exe

Vous pouvez quitter MSYS :

```
$ exit
```

3.2.5 Installation

Ce chapitre traite de l'installation de QEmu sans le module accélérateur (Kqemu). Celui-ci sera abordé dans le chapitre suivant. QEmu fonctionne parfaitement sans ce module, mais les performances seront nettement meilleures s'il est utilisé.

Si vous avez choisi de télécharger une version installable de QEmu, ce chapitre se résume à exécuter ce fichier. Vous pouvez passer au chapitre suivant (paragraphe 3.3, page 11).

Si vous êtes passé par la compilation, voyons comment nous pouvons installer QEmu.

Dans la mesure où QEmu ne fait appel à aucun composant particulier, l'installation se limite à la copie de quelques fichiers.

Nous allons préparer la structure de dossiers pour QEmu. Pour l'exemple, nous partirons d'un dossier créé dans la racine du disque dur, mais tout autre point de départ est valable. Pensez simplement à adapter les chemins.

- Créez, par tout moyen à votre convenance (Explorateur Windows, ligne de commande, etc...), la structure de dossiers suivante :

```
C:\--QEMU
        |
        +--- BIOS
        |
        +--- KQEMU
        |
        `--- IMAGES
```

  Cette structure n'a aucun caractère obligatoire, mais elle va servir de base pour ce document.

  La suite de ce manuel suppose que le répertoire par défaut est C:\QEMU. Dans une invite de commandes, tapez :

```
C:\Documents and Settings\Nom>CD \QEMU
```

```
C:\QEMU>
```

- Copiez, avec l'outil qui vous convient le mieux, dans le répertoire QEMU lui-même les fichiers **C:\MSYS\home\<NomUtilisateur>\qemu\i386-softmmu\qemu.exe** et **C:\MSYS\home\<NomUtilisateur>\qemu\qemu-img.exe** créés au chapitre Compilation des sources.
- Copiez dans le répertoire BIOS les fichiers : bios.bin, vgabios.bin, vgabios-cirrus.bin que vous trouverez dans **C:\MSYS\home\<NomUtilisateur>\qemu\pc-bios**.

  Note : vérifiez de temps à autre la date et l'heure de ces fichiers. Si les fichiers du dossier BIOS sont plus anciens que ceux de **C:\MSYS\home\<NomUtilisateur>\qemu\pc-bios**, remplacez-les par les nouvelles versions.

QEmu est maintenant fonctionnel en tant qu'application. Mais il a encore besoin de quelques fichiers pour pouvoir démarrer. Ce point sera abordé dans le chapitre Démarrage rapide de QEmu (paragraphe 4, page 12).

3.3 Module accélérateur

L'utilisation d'un module accélérateur est totalement facultative, mais dans certains cas, il permet d'augmenter considérablement la vitesse d'exécution de QEmu. Il est donc vivement conseillé de l'installer.

Il existe actuellement deux modules accélérateurs pour QEmu : Kqemu, le module propriétaire de Fabrice BELLARD et qvm86 qui est entièrement libre (http://savannah.nongnu.org/projects/qvm86).

Malheureusement, qvm86 n'a pas été mis à jour depuis juillet 2005, et le patch proposé ne s'applique pas correctement aux sources CVS. De plus, qvm86 ne permet pas pour le moment d'accélérer le code en mode noyau, et est donc moins efficace que Kqemu.

Lorsque le module accélérateur est installé, et que le service est démarré, Kqemu accélère le code qui s'exécute en mode utilisateur. C'est l'option par défaut. Pour accélérer également le code qui s'exécute en mode kernel, il faut ajouter l'option `-kernel-kqemu` à la ligne de commande de QEmu.

Remarque : Certains systèmes d'exploitation peuvent rencontrer des problèmes lorsque Kqemu est activé. Une option de la ligne de commande de QEmu (`-no-kqemu`) permet de désactiver ponctuellement le module.

Le tableau suivant donne une idée de l'influence de kqemu.

SE cible	*Sans kqemu*	*Avec kqemu*	*-kernel-kqemu*
Temps du démarrage de QEmu jusqu'à l'affichage de l'écran de login. Athlon 64 3000+ (1,8 Ghz) – 1 Go RAM			
Windows 2000	35 s	34 s	27 s
Ubuntu 6.06	2 mn 55 s	1 mn 51 s	60 s
Mandriva 2005 LE		2 mn 10 s	1 mn 25 s
Windows 95	13 s	18 s	Ne démarre pas
Temps du démarrage de QEmu jusqu'à l'affichage de l'écran de login. Pentium IV HT 2,8 Ghz – 512 Mo			
Windows 2000	68 s	55 s	35 s
Windows 95	14 s	27 s	Ne démarre pas

On peut voir que les SE 16 bits semblent s'exécuter plus rapidement lorsque Kqemu n'est pas activé.

3.3.1 Télécharger Kqemu

Kqemu est disponible en téléchargement sur la page : http://qemu.org/kqemu-1.3.0pre9.tar.gz.

Attention, ce lien changera lors de la mise en ligne d'une nouvelle version. Rendez-vous ici dans ce cas : http://qemu.org/download.html

Ce fichier étant au format gzip, il vous faudra peut-être télécharger et installer 7zip (entre autres) : http://www.7zip.org.

Décompactez l'archive Kqemu dans le sous-répertoire Kqemu de QEmu. Kqemu est déjà compilé dans sa forme pour Windows : c'est le fichier kqemu.sys.

3.3.2 Installer Kqemu

Pour installer Kqemu, cliquez avec le bouton droit de la souris sur le fichier **Kqemu.inf**, puis sur Installer.

Il est possible de désinstaller Kqemu par l'intermédiaire du panneau de configuration.

Par défaut, le service n'est pas démarré. Pour ce faire, tapez simplement dans une Invite de commandes :

```
C:\QEMU>net start kqemu
```

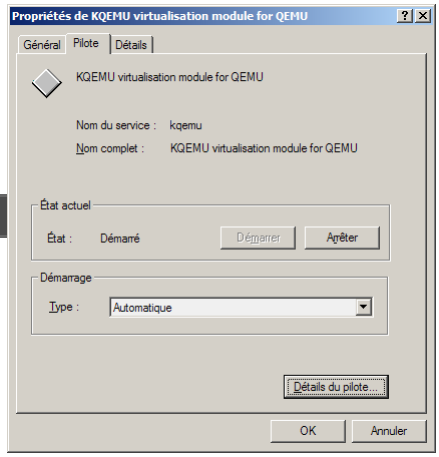


Illustration 2: Propriétés du service

Le service sera actif pendant la session courante, mais il faudra le relancer après un redémarrage de Windows .

Si vous préférez démarrer automatiquement le service au lancement de Windows, ouvrez le Panneau de configuration, icône Système, puis onglet Matériel, bouton Gestionnaire de périphériques. Affichez les périphériques cachés, puis cherchez **Kqemu virtualisation module for QEmu** dans les Pilotes non plug and play. Affichez alors les propriétés, et modifiez le mode de démarrage (--> Automatique). De cette manière, l'accélération sera disponible en permanence. Il est toujours possible de la désactiver ponctuellement, sur la ligne de commande de QEmu (option `-no-kqemu`).

4 Démarrage rapide de QEmu

A partir de ce point, nous allons utiliser principalement la ligne de commande pour configurer et démarrer QEmu. Ouvrez donc une **Invite de commandes** et placez vous dans le dossier C:\QEMU.

Une manière simple d'avoir un aperçu des options de QEmu est de taper :

```
C:\QEMU>qemu
```

Ce qui devrait afficher quelque chose ressemblant à ceci :

```
QEMU PC emulator version 0.8.1, Copyright (c) 2003-2005 Fabrice Bellard
usage: qemu [options] [disk_image]

'disk_image' is a raw hard image image for IDE hard disk 0

Standard options:
-M machine      select emulated machine (-M ? for list)
-fda/-fdb file  use 'file' as floppy disk 0/1 image
-hda/-hdb file  use 'file' as IDE hard disk 0/1 image
-hdc/-hdd file  use 'file' as IDE hard disk 2/3 image
-cdrom file     use 'file' as IDE cdrom image (cdrom is ide1 master)
-boot [a|c|d]   boot on floppy (a), hard disk (c) or CD-ROM (d)
-snapshot       write to temporary files instead of disk image files
-no-quit        disable SDL window close capability
-no-fd-bootchk  disable boot signature checking for floppy disks
-m megs         set virtual RAM size to megs MB [default=128]
-smp n          set the number of CPUs to 'n' [default=1]
-nographic      disable graphical output and redirect serial I/Os to console
-audio-help     print list of audio drivers and their options
-soundhw c1,    enable audio support
                and only specified sound cards (comma separated list)
                use -soundhw ? to get the list of supported cards
                use -soundhw all to enable all of them
-localtime      set the real time clock to local time [default=utc]
-full-screen    start in full screen
```

```
-win2k-hack     use it when installing Windows 2000 to avoid a disk full bug
-usb            enable the USB driver (will be the default soon)
-usbdevice name add the host or guest USB device 'name'

Network options:
-net nic[,vlan=n][,macaddr=addr][,model=type]
                create a new Network Interface Card and connect it to VLAN 'n'
-net user[,vlan=n][,hostname=host]
                connect the user mode network stack to VLAN 'n' and send
                hostname 'host' to DHCP clients
-net tap[,vlan=n],ifname=name
                connect the host TAP network interface to VLAN 'n'
-net socket[,vlan=n][,fd=h][,listen=[host]:port][,connect=host:port]
                connect the vlan 'n' to another VLAN using a socket connection
-net socket[,vlan=n][,fd=h][,mcast=maddr:port]
                connect the vlan 'n' to multicast maddr and port
-net none       use it alone to have zero network devices; if no -net option
                is provided, the default is '-net nic -net user'

-tftp prefix    allow tftp access to files starting with prefix [-net user]
-redir [tcp|udp]:host-port:[guest-host]:guest-port
                redirect TCP or UDP connections from host to guest [-net user]

Linux boot specific:
-kernel bzImage use 'bzImage' as kernel image
-append cmdline use 'cmdline' as kernel command line
-initrd file    use 'file' as initial ram disk

Debug/Expert options:
-monitor dev    redirect the monitor to char device 'dev'
-serial dev     redirect the serial port to char device 'dev'
-parallel dev   redirect the parallel port to char device 'dev'
-pidfile file   Write PID to 'file'
-S              freeze CPU at startup (use 'c' to start execution)
-s              wait gdb connection to port 1234
-p port         change gdb connection port
-d item1,...    output log to /tmp/qemu.log (use -d ? for a list of log items)
-hdachs c,h,s[,t]  force hard disk 0 physical geometry and the optional BIOS
                translation (t=none or lba) (usually qemu can guess them)
-L path         set the directory for the BIOS and VGA BIOS
-kernel-kqemu   enable KQEMU full virtualization (default is user mode only)
-no-kqemu       disable KQEMU kernel module usage
-std-vga        simulate a standard VGA card with VESA Bochs Extensions
                (default is CL-GD5446 PCI VGA)
-no-acpi        disable ACPI
-no-reboot      exit instead of rebooting
-loadvm file    start right away with a saved state (loadvm in monitor)
-vnc display    start a VNC server on display
-option-rom rom load a file, rom, into the option ROM space

During emulation, the following keys are useful:
ctrl-alt-f      toggle full screen
ctrl-alt-n      switch to virtual console 'n'
ctrl-alt        toggle mouse and keyboard grab

When using -nographic, press 'ctrl-a h' to get some help.
```

Bon, plutôt indigeste, au premier abord, mais ça donne une bonne idée de ce que QEmu est capable de faire..

Commençons par les options essentielles à l'utilisation de l'émulateur. Nous verrons les autres plus tard.

4.1 Les périphériques de stockage

Tout ordinateur normalement constitué (je ne parle pas des clients légers) possède au moins un disque dur et un lecteur de CD. QEmu simule ces périphériques en utilisant des fichiers enregistrés sur votre disque dur.

Dans certains cas, QEmu est capable d'utiliser les périphériques physiques présents sur votre ordinateur. Ce point est abordé plus loin, dans le paragraphe traitant des Périphériques physiques (paragraphe 4.1.2, page 14).

Le périphérique virtuel le plus important est probablement le disque dur. Voyons comment le mettre en place.

4.1.1 Créer un disque dur virtuel

Rappel : les lignes de commandes utilisées dans la suite du document supposent que le répertoire par défaut est C:\QEMU.

Pour vous placer dans ce répertoire :

```
C:\>cd \QEMU
C:\QEMU>
```

Remarque : pour les plus jeunes, qui ne sont pas familiers de la ligne de commande, `C:\QEMU>` est l'invite de commande. Ce texte ne doit pas être tapé car il ne fait pas partie de la commande elle-même. Le premier caractère utile est celui qui suit `>`.

Pour créer rapidement une image de disque dur, utilisez la commande suivante :

```
C:\QEMU>qemu-img create -f qcow2 IMAGES\DISQUEDUR.IMG 10G
```

Après exécution de cette commande, vous devriez avoir un fichier DISQUEDUR.IMG dans le dossier IMAGES, pesant quelques dizaines de kilo-octets. Cela est normal, rassurez-vous, la capacité du disque virtuel est bien de 10 Go, même s'il n'occupe que très peu de place pour le moment.

4.1.2 Les périphériques physiques

Si, pour le disque dur virtuel, il est préférable de s'en tenir à un fichier image (qui apporte d'autres avantages abordés plus loin), il est parfois long et pénible d'être obligé de transformer d'abord un CD en image ISO avant de pouvoir l'utiliser avec QEmu.

Heureusement, QEmu gère très bien les disquettes et CD réels.

Le nom du fichier image de disquette peut être remplacé par **\\.\A:** ou **//./A:** dans la ligne de commande de QEmu. La même syntaxe s'applique aux lecteurs de CD. Utilisez les lettres attribuées par Windows (ex. \\.\D:).

Remarque : La disquette est accessible en lecture et en écriture, offrant une première possibilité d'échange de fichiers entre l'hôte et la machine virtuelle.

4.2 Installation d'un système d'exploitation dans QEmu

Maintenant que nous avons mis en place l'environnement nécessaire, nous allons enfin pouvoir démarrer QEmu, et profiter de notre « *PC dans le PC* ».

Mais, au point où nous sommes arrivés, nous n'avons encore qu'un PC vierge, sans système d'exploitation (SE). Tout le matériel est installé, mais de logiciel, point encore...

Deux options s'offrent à nous :

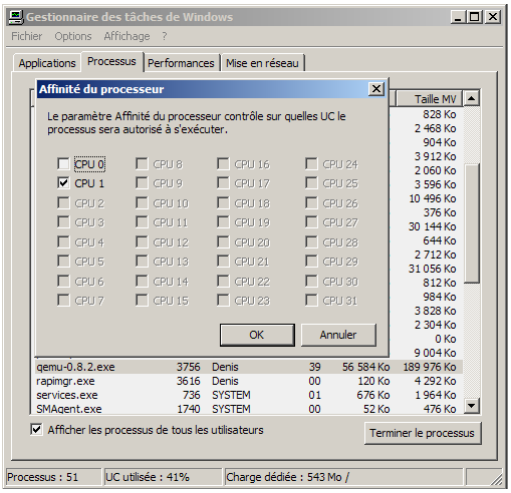
- Télécharger une image disque déjà préparée. Plusieurs sites proposent des images disques pour QEmu. Il faut noter, cependant, que seuls les SE libres peuvent être téléchargés de la sorte. Les SE commerciaux (Windows, MacOS, etc...) sont soumis à licence et ne peuvent être mis à disposition gratuitement.
- Installer soi-même un SE, comme on le ferait sur un PC réel. Il faut, dans ce cas, outre les CD d'installation, posséder également la licence du logiciel, cela va de soi.

4.2.1 Processeur hôte à coeurs multiples

Nous allons bientôt lancer notre première machine virtuelle, mais avant, il faut encore éliminer une dernière source potentielle d'ennuis.

Les processeurs à coeurs multiples (Pentium HT, Pentium D, AMD X2) rendent QEmu instable et provoquent soient le blocage complet du système hôte, soit son redémarrage pur et simple.

La parade consiste à forcer l'exécution de qemu.exe sur un seul coeur. Ceci peut être fait de deux manières.


Gestionnaire des tâches de Windows
Fichier Options Affichage ?
Applications Processus Performances Mise en réseau
Affinité du processeur
Le paramètre Affinité du processeur contrôle sur quelles UC le processus sera autorisé à s'exécuter.
CPU 0 CPU 1 CPU 2 CPU 3 CPU 4 CPU 5 CPU 6 CPU 7
CPU 8 CPU 9 CPU 10 CPU 11 CPU 12 CPU 13 CPU 14 CPU 15
CPU 16 CPU 17 CPU 18 CPU 19 CPU 20 CPU 21 CPU 22 CPU 23
CPU 24 CPU 25 CPU 26 CPU 27 CPU 28 CPU 29 CPU 30 CPU 31
OK
Annuler
Taille MV
qemu-0.8.2.exe 3756 Denis 39 56 584 Ko 189 976 Ko
rapimgr.exe 3616 Denis 00 120 Ko 4 292 Ko
services.exe 736 SYSTEM 01 676 Ko 1 964 Ko
SMAgent.exe 1740 SYSTEM 00 52 Ko 476 Ko
Afficher les processus de tous les utilisateurs
Terminer le processus
Processus : 51
UC utilisée : 41%
Charge dédiée : 543 Mo /

– Le choix de l'affinité d'un processus peut être fait avec le Gestionnaire de tâches de Windows, en cliquant avec le bouton droit de la souris sur la ligne du processus qemu.exe (onglet Processus), puis en prenant l'option Définir l'affinité. Il suffit alors de ne cocher qu'un seul processeur.

  Si QEmu plante avant que ne puissiez faire cette manipulation, utilisez l'option `-S` de la ligne de commande (Chapitre Autres options de la ligne de commande, paragraphe 5.2.6, page 29).

  Remarque : Cette opération doit être répétée à chaque lancement de QEmu.

– L'utilitaire imagecfg permet d'inscrire l'affinité directement dans le fichier qemu.exe. Cette opération devra être faite après chaque nouvelle compilation. Cet outil Microsoft peut-être trouvé sur le CD de Windows NT 4.0. Mais une petite recherche avec Google vous permettra de le télécharger très rapidement aussi. Voyez la section Utilitaires divers pour le mode d'emploi (paragraphe 6, page 34).

Remarque : depuis la version 0.8.2 CVS 14-07-2005, l'affinité est définie automatiquement pour un seul processeur lors de la compilation.

4.2.2 Télécharger des images pré-installées

Un site très proche de QEmu propose bon nombre d'images de différents SE libres. Il s'agit du Free OS Zoo (http://www.oszoo.org/wiki/index.php/Main_Page). Pour vous rendre directement à la page de téléchargement des images : http://www.oszoo.org/wiki/index.php/Category:OS_images. Encore une fois, ce site ne propose que des SE **libres**.

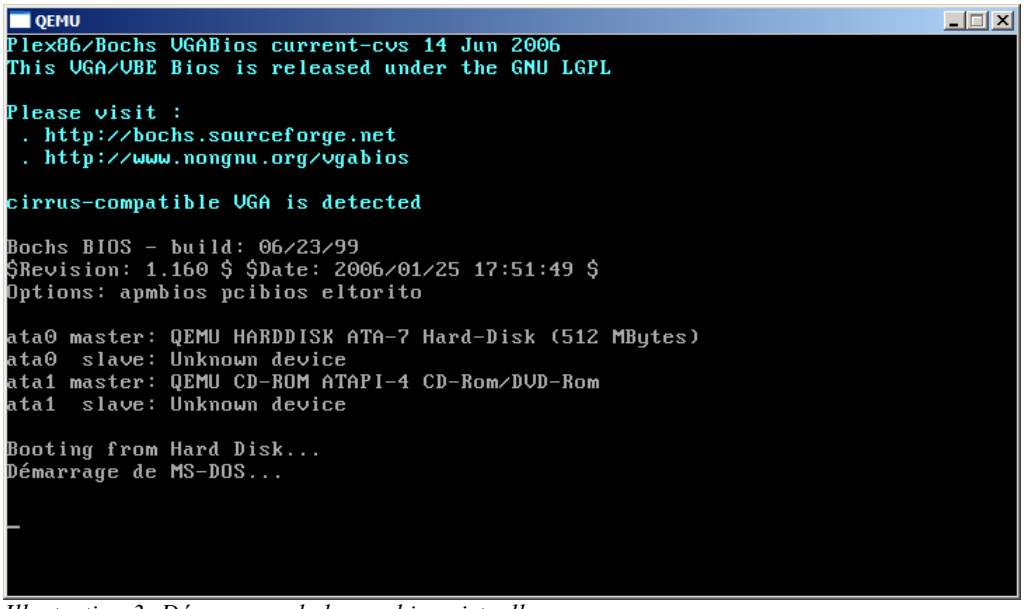
Mais en cherchant sur le Web, vous pourrez probablement trouver d'autres sites proposant des images pour QEmu.

Une fois l'image téléchargée, il suffit de la placer dans le répertoire IMAGES créé précédemment et de taper ensuite la ligne de commande :

```
C:\QEMU>qemu -hda IMAGES\<NomDeLImage> -m 192 -localtime -L BIOS
```

Cette ligne de commande (minimaliste, il y a beaucoup d'autres options) va démarrer une machine virtuelle avec comme premier disque dur l'image <NomDeLImage> et pourvue de 192 Mo de RAM. Le paramètre `-localtime` permet simplement de caler l'horloge de la machine virtuelle sur celle de la machine hôte. Le paramètre `-L` indique à QEmu dans quel dossier il doit chercher le BIOS.

Voici, par exemple, le démarrage QEmu sous MS-DOS 6.22.


QEMU
Plex86/Bochs VGABios current-cvs 14 Jun 2006
This VGA/VBE Bios is released under the GNU LGPL
Please visit :
. http://bochs.sourceforge.net
. http://www.nongnu.org/vgabios
cirrus-compatible VGA is detected
Bochs BIOS - build: 06/23/99
$Revision: 1.160 $ $Date: 2006/01/25 17:51:49 $
Options: apmbios pcibios eltorito
ata0 master: QEMU HARDDISK ATA-7 Hard-Disk (512 MBytes)
ata0 slave: Unknown device
ata1 master: QEMU CD-ROM ATAPI-4 CD-Rom/DVD-Rom
ata1 slave: Unknown device
Booting from Hard Disk...
Démarrage de MS-DOS...
Illustration 3: Démarrage de la machine virtuelle

Pour terminer la machine virtuelle (éteindre le PC virtuel, en quelque sorte) :

– Si le SE sait arrêter automatiquement le PC, quittez simplement le SE. La fenêtre QEmu disparaîtra d'elle-même.

– Sinon, fermez la fenêtre QEmu avec la croix rouge.

4.2.3 Installer soi-même son système

Cette procédure s'apparente en tous points à l'installation d'un SE sur un PC réel. Il vous faut :

- les disquettes et/ou CD d'installation. A défaut des supports physiques, des images ISO feront parfaitement l'affaire ;
- les clés de licences, si nécessaire ;
- le mode d'emploi de l'installation du SE (si vous ne savez pas par où commencer, ce n'est pas QEmu qui vous l'apprendra). Il faut savoir sur quel support le PC doit démarrer pour lancer l'installation (disquette ou CD)
- du temps et de la patience : installer un SE dans un émulateur est souvent plus long que sur un matériel réel. QEmu n'est pas encore totalement stable, et la phase d'installation est généralement plus délicate que la phase d'utilisation (la détection du matériel par les programmes d'installation est souvent *agressive*, et peut générer des problèmes). Il est parfois nécessaire de désactiver le module accélérateur pendant l'installation.

  Quoi qu'il en soit, la liste des SE s'installant et tournant correctement dans QEmu est déjà très impressionnante (voyez sur Free OS Zoo).

Nous allons faire une installation à partir des supports réels, nous évitant ainsi l'étape de création d'images ISO à partir de ces supports (ce qui peut être assez long pour un DVD).

Insérez maintenant les supports nécessaires à l'installation dans les lecteurs appropriés.

La ligne de commande de QEmu va dépendre du support de démarrage. Prenons l'exemple pour un CD bootable :

```
C:\QEMU>qemu -hda IMAGES\<NomDeLImage> -m 192 -localtime -L BIOS -cdrom \\.\D:
-boot d
```

<NomDeLImage> est une image de disque dur vierge, créée avec qemu-img.

`-m 192` permet d'ajuster la quantité de mémoire vive (RAM) installée dans la machine virtuelle. A adapter en fonction des besoins du SE cible.

`-cdrom \\.\D:` indique à QEmu de prendre le lecteur hôte D: comme lecteur de CD. Si le lecteur de CD hôte porte un autre nom, modifiez en conséquence.

`-boot d` fait démarrer le PC virtuel sur le lecteur de CD. Pour démarrer sur la disquette, spécifiez **`-boot a`** et ajoutez `-fda \\.\A:`.

Remarque : en général, à la fin de l'installation, le PC doit redémarrer. Ici, QEmu posera un petit problème dans la mesure où il ne permet pas de changer de **périphérique de démarrage**. Le `-boot` indiqué lors du lancement pour l'installation ne peut être changé sans arrêter QEmu.

Windows 2000 et XP s'en tireront correctement car ils affichent le message : *`Appuyez sur n'importe quelle touche pour démarrer à partir du CD`*. Il suffit d'attendre quelques secondes pour que QEmu continue à partir du disque dur. Pour les autres SE, il faudra *tuer* QEmu, puis le relancer sans l'option `-boot`, sinon il vont redémarrer à partir du CD et relancer leur procédure d'installation.

Le plus simple est alors de retirer le CD du lecteur de l'hôte lorsque le message demandant le redémarrage est affiché, puis de laisser redémarrer la machine virtuelle. QEmu se plaindra alors de ne pas pouvoir démarrer à partir du CD. Il suffit de le tuer à ce moment là.

Entrez à nouveau la ligne de commande, sans les options de CD ni de boot :

```
C:\QEMU>qemu -hda IMAGES\<NomDeLImage> -m 192 -localtime -L BIOS
```

C'est cette même ligne de commande qui permettra par la suite de démarrer la machine virtuelle lorsque vous voudrez l'utiliser.

Remarque : Ce problème peut maintenant être contourné de manière plus élégante avec l'option `-no-reboot`. (voir paragraphe 5.2.6, page 30)

Si le SE cible demande une combinaison de touches du style Ctrl-Alt-Suppr pour ouvrir une session, passez en mode moniteur (**Ctrl-Alt-2** - voir le chapitre Installer des applications dans le SE – paragraphe 4.3, page 18 - pour une présentation rapide du mode moniteur), puis tapez :

```
QEMU 0.8.1 monitor - type 'help' for more information
(qemu) sendkey ctrl-alt-delete
```

Tapez **Ctrl-Alt-1** pour revenir à l'écran principal.

Au niveau de sa ligne de commandes, QEmu identifie les périphériques virtuels à la manière de Linux : `fda`, `fdb` pour les lecteurs de disquettes (floppy disk) ; `hda`, `hdb`, `hdc`, `hdd` pour les lecteurs de disques durs (hard disk).

Le lecteur de CD est le périphérique maître sur le second contrôleur IDE. Il prend la place de `hdc`. Les paramètres `-hdc` et `-cdrom` s'excluent donc mutuellement.

Attention : si vous ajoutez l'option `-cdrom \\.\X:` à la ligne de commande, mais que le lecteur hôte ne contient pas de support, QEmu refusera de démarrer. Même si vous ne précisez pas cette option, le lecteur de CD sera disponible sur la machine virtuelle (sauf si vous avez utilisé `-hdc`). Voyez plus loin les commandes du moniteur (paragraphe 5.3, page 30) pour savoir comment insérer ou changer un CD dans le lecteur de la machine virtuelle.

Utilisez autant que possible le module accélérateur (Kqemu). Il est toutefois possible que les SE 16 bits (MS-DOS, Windows 9x) soient moins rapides lorsque Kqemu est activé. Dans ce cas, ou si celui-ci provoque des erreurs, ajoutez le paramètre `-no-kqemu` à la ligne de commande de QEmu avant de le relancer. L'accélérateur sera désactivé, mais l'émulation sera moins rapide.

Remarque : Depuis la version 1.3.0pre9 de Kqemu, l'option `-kernel-kqemu` est utilisable sur un hôte Windows XP, pour la plupart des systèmes cibles (DOS, Windows 2000, Linux (Ubuntu, Mandriva) démarrent. Windows 9x plante). Utilisez la si possible, car elle améliore encore les performances de l'émulateur.

4.2.4 Remarques

4.2.4.1 Capture de la souris

Pour que les mouvements de la souris soient transmis au SE cible, il faut d'abord cliquer dans la fenêtre de QEmu. A partir de ce moment, la souris reste *prisonnière* de la fenêtre QEmu. Si le SE cible ne reconnaît pas la souris, vous aurez l'impression que celle-ci a disparu. Pour la libérer, il faut appuyer simultanément sur les touches Ctrl et Alt du clavier (c'est indiqué dans la barre de titre de QEmu).

Une option très intéressante, si le SE cible possède le pilote adéquat (sinon, il faudra en installer un), est `-usbdevice`

`tablet`. Cette option ajoute une tablette USB à la machine virtuelle QEmu, ce qui, en soi, ne présente pas forcément un intérêt majeur, mais permet surtout à la souris de ne plus être bloquée à la frontière de la fenêtre QEmu. Ctrl-Alt n'est plus nécessaire.

4.2.4.2 Utilisation élevée du processeur

Certains SE un peu anciens (MS-DOS, Windows 9x, etc...) souffrent d'un petit défaut de conception qui se traduit par une utilisation intense du processeur hôte, même lorsque le SE cible ne fait rien. Ce problème n'est pas dû à l'émulateur, mais est inhérent au système d'exploitation cible lui-même (lorsque ce SE tourne sur une machine réelle, il provoque les mêmes effets). Si vous démarrez le Gestionnaire de tâches de Windows (Ctrl-Maj-Echap), vous verrez alors que le processeur est occupé à 100%, la plus grande partie étant consommée par QEmu lui-même.

- Sous MS-DOS (ou équivalent), il est maintenant possible d'installer le pilote POWER.EXE. Si celui-ci provoque le blocage de la machine virtuelle, essayez d'installer DOSIDLE (http://www.vmware.com/software/dosidle210.zip)
- Sous Windows 9x, un utilitaire équivalent peut-être trouvé ici : http://www.user.cityline.ru/~maxamm/amnhltm.zip.

Windows NT et ses suivants, Linux et la plupart des autres SE récents n'ont pas ce défaut.

4.2.5 Interfaces graphiques

Lorsqu'on expérimente beaucoup avec QEmu, il devient vite pénible de taper et retaper des lignes de commandes. QEmu ne possède pas pour le moment d'interface graphique intégrée, mais il existe plusieurs utilitaires permettant de mémoriser tous les paramètres nécessaires à une machine virtuelle, pour la démarrer ensuite en quelques clics.

Dans l'absolu, ces outils ne font que créer une ligne de commande à partir des informations choisies par l'utilisateur.

JQEMU : http://www.exprofesso.com/jqemu/, une interface en Java.

QGUI : http://perso.wanadoo.es/comike/, ne fonctionne plus avec les dernières versions de QEmu, car la ligne de commande a changé.

4.3 Installer des applications dans le SE cible

Installer une application à partir d'un CD ou d'une disquette (?) ne présente pas plus de difficultés que sur un PC réel. Si l'installation doit se faire à partir d'un CD, le SE cible doit bien sûr reconnaître le lecteur de CD virtuel, les pilotes nécessaires doivent être installés.

La machine virtuelle étant lancée, et le SE cible chargé, QEmu ne reconnaît pas automatiquement l'insertion d'un CD dans le lecteur de l'hôte. Heureusement, tout est prévu.

Pour indiquer à QEmu (et au système cible) qu'un nouveau support a été inséré, nous allons passer en mode Moniteur. Dans ce mode, il est possible d'exécuter des commandes pour modifier l'état de la machine virtuelle, ou obtenir des informations sur son fonctionnement. Le moniteur est décrit plus loin dans ce document (paragraphe 5.3, page 30).

Pour atteindre la fenêtre du moniteur, il faut appuyer simultanément sur les touches **Ctrl-Alt-2**. Pour revenir à l'écran principal de QEmu, tapez **Ctrl-Alt-1.**

Remarque : lorsqu'on bascule vers le moniteur, le premier caractère tapé au clavier n'est pas pris en compte...

```
QEMU 0.8.1 monitor - type 'help' for more information
(qemu)
```

Pour insérer notre CD dans la machine virtuelle, il suffit de taper :

```
(qemu) change cdrom //./d:
```

en admettant, bien sûr, que le lecteur physique (hôte) porte la lettre D:. Le voyant du lecteur de CD doit s'allumer brièvement. Si le CD est configuré pour le lancement automatique, et que le SE cible prend cette fonction en charge, il démarrera tout seul dans la machine virtuelle.

Tapez ensuite **Ctrl-Alt-1** pour revenir à l'écran principal.

Cette commande fonctionne de la même manière pour un changement de disquette.

```
(qemu) change fda //./a:
```

Si vous souhaitez simplement éjecter le CD (ou la disquette) du lecteur virtuel :

```
(qemu) eject cdrom
(qemu) eject fda
```

Éjectez toujours le support du lecteur virtuel avant de le sortir du lecteur physique (le SE cible ne détectera pas automatiquement que le média a été retiré du lecteur physique). Cette éjection peut être faite depuis le SE cible, QEmu la détectera (il n'est pas nécessaire d'employer la commande `eject` du moniteur.

Bien entendu, les spécifications de lecteurs physiques (//./x:) peuvent être remplacées par des noms d'images.

5 Utilisation avancée

Le chapitre précédent nous a permis de démarrer rapidement notre première machine virtuelle en utilisant quelques unes des options de QEmu. Mais il y en a bien d'autres. En voici une présentation un peu plus complète.

5.1 Images disques – options avancées

QEmu simule deux contrôleurs IDE, et peut donc utiliser jusqu'à quatre disques durs virtuels (trois si le lecteur de CD est utilisé).

qemu-img est l'outil dédié à la création d'images de disques. Il permet de créer le fichier qui servira de disque dur à la machine virtuelle.

Voici toutes les options possibles pour qemu-img.

```
C:\QEMU>qemu-img
qemu-img version 0.8.2, Copyright (c) 2004-2006 Fabrice Bellard
usage: qemu-img command [command options]
QEMU disk image utility

Command syntax:
  create [-e] [-b base_image] [-f fmt] filename [size]
  commit [-f fmt] filename
  convert [-c] [-e] [-f fmt] filename [-O output_fmt] output_filename
  info [-f fmt] filename

Command parameters:
  'filename' is a disk image filename
  'base_image' is the read-only disk image which is used as base for a copy on
    write image; the copy on write image only stores the modified data
  'fmt' is the disk image format. It is guessed automatically in most cases
  'size' is the disk image size in kilobytes. Optional suffixes 'M' (megabyte)
    and 'G' (gigabyte) are supported
  'output_filename' is the destination disk image filename
  'output_fmt' is the destination format
  '-c' indicates that target image must be compressed (qcow format only)
  '-e' indicates that the target image must be encrypted (qcow format only)

Supported format: qcow2 vvfat vpc bochs dmg cloop vmdk qcow host_device raw
```

qemu-img comprend quatre commandes.

– `create` : permet de créer un fichier image.

  Créer une image de disquette vierge :

```
C:\QEMU>qemu-img create -f qcow2 IMAGES\Floppy.img 1440
```

- `commit` : les informations du fichier image `filename` sont écrites dans l'image de base.

  ATTENTION : si une image de base est utilisée pour plusieurs autres images, n'appliquez cette commande qu'à une seule image, sous peine de rendre l'image de base inutilisable. Il est alors fort probable que les autres images dépendant de cette image de base devront être réinitialisées.
- `convert` : permet de créer une nouvelle image à partir d'une image existante, en changeant éventuellement le format.
- `info` : affiche des informations sur l'image spécifiée.

5.1.1 Les différents formats d'images

5.1.1.1 Le format raw

Ce format permet de créer une image de 2 Go maximum (jusqu'à la version 0.8.1 de qemu-img). Le fichier d'une image raw consomme immédiatement de la place sur le disque dur de l'hôte. Autrement dit, une image d'1 Go, par exemple, mobilisera 1 Go sur le disque dur, même si le système cible n'en utilise que 200 Mo...

Ce format a l'avantage d'être compatible avec d'autres émulateurs.

Exemple :

```
C:\QEMU>qemu-img create -f raw IMAGES\DisqueRAW.img 100M
```

crée une image de type raw de 100 Mo

Remarque : la version 0.8.2 fait disparaître la limite des 2 Go.

5.1.1.2 Le format qcow2

Qcow2, qui a fait son apparition avec la version 0.8.3, est de loin le format le plus intéressant. C'est le format que nous avons déjà rencontré lors du démarrage rapide. Il a l'avantage de n'utiliser que l'espace réellement nécessaire. Une image de 10 Go, par exemple, ne pèse que quelques Ko lors de sa création. Cette image va grandir au fur et à mesure que le SE cible écrit ses fichiers. En fin d'installation, une image Windows 2000, par exemple, fait environ 700 à 800 Mo. Mais les 9 Go restants pourront être utilisés par la suite.

Ce format permet également de comprimer et de crypter une image. Le support des *instantanés multiples* est pris en charge à partir de ce format (paragraphe 5.3.7, page 33).

Exemple :

```
C:\QEMU>qemu-img create -f qcow2 IMAGES\DisqueCOW.img 10G
```

crée une image de type qcow2 de 10 Go.

Remarque : le format précédent, `qcow,` est conservé pour des raisons de compatibilité.

5.1.1.3 Les autres formats

QEmu sait créer et utiliser d'autres formats d'images. Ceux-ci sont utiles surtout lorsqu'on travaille simultanément avec d'autres émulateurs.

- vpc : image pour VirtualPC (Microsoft http://www.microsoft.com/france/windows/xp/virtualpc/default.mspx)
- bochs : l'émulateur de PC Bochs (http://bochs.sourceforge.net)
- dmg : image disque sous Mac OSX
- cloop : image Loop compressée (Linux)
- vmdk : image pour le virtualiseur VMWare (http://www.vmware.com)

5.1.2 Les images de base

Nous avons déjà vu que le format cow présente des avantages d'un point de vue occupation de l'espace disque. Voyons maintenant une autre caractéristique très intéressante de ce format.

Avec l'option `-b`, qemu-img permet de créer une image basée sur une autre image existante.

Imaginons que nous venons d'installer Windows 2000 dans une image nommée DD_W2K.IMG. Maintenant que cette image est paramétrée comme il faut, tous les éléments utiles ont été installés et configurés dans le SE cible, nous aimerions utiliser cette images pour toute une série de tests. Et après chaque test, nous voulons repartir d'une image propre. Eh bien, le format qcow permet de faire ce genre de manipulation très facilement, et réinitialiser l'image ne prend pas plus de temps qu'il n'en faut pour taper une ligne de commande qemu-img.

COW signifie Copy On Write, c'est à dire Copie lors de l'écriture. Autrement dit, QEmu peut lire dans une image, tout en écrivant dans une autre. Mais ces deux images sont vues comme ne faisant qu'une seule. C'est ici qu'intervient l'image de base, option `-b` de qemu-img.

Pour la démonstration, nous allons renommer notre image Windows 2000 toute neuve en DD_W2K_BASE.IMG.

Ensuite, créons une nouvelle image avec la commande `create`, comme suit :

```
C:\QEMU>qemu-img create -b IMAGES\DD_W2K_BASE.IMG -f qcow2 IMAGES\DD_W2K.IMG
Formating 'images\dd_w2k.img', fmt=qcow, backing_file=images\dd_w2k_base.img,
size=nnnnnnn kB
```

Nous avons maintenant une nouvelle image (que nous appellerons *image différentielle*, puisqu'elle ne contient que les différences par rapport à l'image de base), de quelques Ko en taille réelle, mais dont la taille virtuelle est identique à celle de l'image de base.

Lorsque nous lancerons QEmu :

```
C:\QEMU>qemu -hda IMAGES\dd_w2k.img -m 192 -localtime -L BIOS
```

celui-ci ira lire dans l'image IMAGES\dd_w2k_base.img, MAIS, toutes les écritures seront faites dans IMAGES\dd_w2k.img. L'image de base reste inchangée. Un secteur non modifié est lu à partir de l'image de base, un secteur modifié (récrit) est lu à partir de *l'image différentielle*.

Ainsi, pour retrouver notre Windows de départ, après un test, il suffit de recréer *l'image différentielle* dd_w2k.img, par la même ligne de commande que précédemment.

De plus, plusieurs *images différentielles* peuvent utiliser la même image de base, puisque celle-ci est en lecture seule.

Remarques :

- L'image de base peut-être au format raw.
- Il est possible d'intégrer tous les changements d'une image différentielle dans l'image de base avec la commande :

  ```
  C:\QEMU>qemu-img commit -f qcow2 IMAGES\dd_w2k.img
  ```

  Remarque : La commande `commit` du moniteur ne s'applique que si QEmu a été démarré avec l'option `-snapshot`. Dans ce cas, les secteurs de *l'image temporaire automatique* sont transférés vers l'image de base.

  ATTENTION : si une même image de base est utilisée pour plusieurs images différentielles, n'appliquez cette commande qu'à une seule image, sous peine de rendre l'image de base inutilisable. Il est alors fort probable que les autres images différentielles dépendant de cette image de base devront être réinitialisées.

5.1.3 Autres commandes

La commande `info` permet d'afficher des renseignements sur l'image disque.

```
C:\QEMU>qemu-img info IMAGES\dd_w2k.img
image: dd_w2k.img
file format: qcow2
virtual size: 5.0G (5368709120 bytes)
disk size: 482M
cluster_size: 4096
```

```
Snapshot list:
ID        TAG                 VM SIZE                DATE       VM CLOCK
1         SAVE1                   45M aaaa-mm-jj hh:mm:ss   hh:mm:ss.mmm
2         SAVE2                   45M aaaa-mm-jj hh:mm:ss   hh:mm:ss.mmm
```

La commande `convert` permet de passer d'un format d'image à un autre. Lors de la conversion, seuls les secteurs utilisés sont récrits, permettant par la même occasion de réduire la taille du fichier image. Il est bien sûr possible d'avoir des formats source et destination identiques.

Exemple :

```
C:\QEMU>qemu-img convert -f qcow2 IMAGES\dd_w2k.img -O qcow2
IMAGES\dd_w2k_new.img
```

Cette commande copie une image disque en en retirant les secteurs inutilisés.

Remarque : à l'usage, il semble que la syntaxe exacte de la commande `convert` est :

```
qemu-img convert -O <format> <ancienne image> <nouvelle image>
```

5.2 La ligne de commande

Nous avons déjà vu, dans les chapitres précédents quelques unes des options de QEmu. En voici un parcours plus détaillé. Toutes les options ne sont pas présentées, nous nous limiterons aux plus utiles.

5.2.1 Support réseau

QEmu peut émuler une ou plusieurs cartes réseau. Les cartes émulées sont des modèles 10 Mbit/s, mais ceci est amplement suffisant pour un système virtuel. Ces interfaces permettent à QEmu de communiquer avec le monde extérieur, et en premier lieu avec le système hôte. La création d'un VLAN permet également de construire un réseau entre les machines virtuelles. Cette option pose toutefois encore quelques problèmes de fonctionnement sur un hôte Windows.

L'option complète permettant de créer une carte réseau est :

`-net nic[,macaddr=xx:xx:xx:xx][,model=<type>]`

Les options `macaddr` et `type` sont facultatives.

Les valeurs possibles pour `<type>` sont : `ne2k_pci`, `ne2k_isa`, `rtl8139`, `smc91c111`, `lance`. Si `<type>` n'est pas précisé, `ne2k_pci` est pris par défaut. Cette option peut être répétée autant de fois qu'il faut de cartes réseau dans le système cible, mais il faut prendre soin de donner une adresse MAC différente à chaque carte (option `macaddr=xx:xx:xx:xx` avec `52:54:00:12:34:56` comme valeur par défaut).

Lorsqu'aucune option réseau n'est fournie à QEmu, il crée **par défaut** une carte réseau PCI à base de circuit RTL8029 (`ne2k_pci`). L'option par défaut est en réalité : `-net nic -net user`.

Pour interdire la création de la carte réseau, il faut ajouter l'option `-net none` à la ligne de commande.

5.2.1.1 Architecture réseau de QEmu

L'émulation réseau de QEmu peut être implémentée de deux manières.

Le premier mode, le mode utilisateur (user mode) fonctionne correctement sur un hôte Windows, sans élément supplémentaire. Dans ce cas, QEmu se comporte comme n'importe quelle application faisant appel au réseau, utilisant le matériel et les composants réseau existants.

Le second mode, TUN/TAP, est plus spécifique au monde Linux, mais peut être implémenté sous Windows à condition d'installer le logiciel nécessaire. Dans ce mode QEmu crée une carte réseau virtuelle sur l'hôte, où elle peut être configurée comme n'importe quel autre périphérique. Ce mode nécessite les droits d'administration sur l'hôte, puisqu'un périphérique (virtuel) doit être créé.

5.2.1.1.1 Mode utilisateur

Dans ce mode, qui est d'ailleurs le mode par défaut, QEmu ne se contente pas d'émuler la carte réseau de l'ordinateur virtuel, mais il intègre également un pare-feu/passerelle, un serveur DHCP, un serveur DNS et un serveur SMB. Ces éléments ne sont toutefois pas paramétrables.

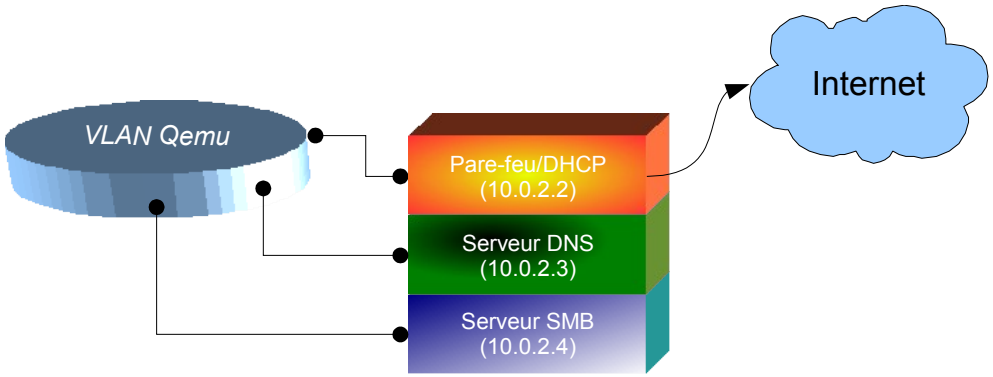


Illustration 4: Architecture réseau

Après l'installation du SE cible, vous pouvez vérifier le bon fonctionnement de la carte réseau virtuelle et de la couche TCP/IP en tapant :

```
ping 10.0.2.2
```

dans une invite de commande ou un terminal du SE cible. Vous devriez obtenir quelque chose ressemblant à ceci :

```
Envoi d'une requête 'ping' sur 10.0.2.2 avec 32 octets de données :

Réponse de 10.0.2.2 : octets=32 temps<1ms TTL=128
Réponse de 10.0.2.2 : octets=32 temps<1ms TTL=128
Réponse de 10.0.2.2 : octets=32 temps<1ms TTL=128
Réponse de 10.0.2.2 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.0.2.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Dans la plupart des cas, il suffit de configurer le protocole TCP/IP de la machine virtuelle pour utiliser DHCP, et tous les autres paramètres se mettent en place automatiquement. Par défaut, la machine virtuelle se verra attribuer l'adresse 10.0.2.15.

Voici, par exemple, la configuration réseau de Windows 2000 sous QEmu :

```
C:\>ipconfig/all

Configuration IP de Windows 2000

     Nom de l'hôte . . . . . . . . . . . : QEMU-W2K
     Suffixe DNS principal . . . . . . . :
     Type de noeud . . . . . . . . . . . : Diffuser
     Routage IP activé . . . . . . . . . : Oui
     Proxy WINS activé . . . . . . . . . : Non

Ethernet carte Connexion au réseau local :

     Suffixe DNS spéc. à la connexion. :
     Description . . . . . . . . . . . . : Carte Realtek PCI Ethernet à base
RTL8029(AS)
     Adresse physique. . . . . . . . . . : 52-54-00-12-34-56
```

```
    DHCP activé . . . . . . . . . . . : Oui
    Autoconfiguration activée . . . . : Oui
    Adresse IP. . . . . . . . . . . . : 10.0.2.15
    Masque de sous-réseau . . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . . : 10.0.2.2
    Serveur DHCP. . . . . . . . . . . : 10.0.2.2
    Serveurs DNS. . . . . . . . . . . : 10.0.2.3
    Bail obtenu . . . . . . . . . . . : mardi 4 juillet 2006 08:16:27
    Bail expire . . . . . . . . . . . : mercredi 5 juillet 2006 08:16:27
```

5.2.1.1.2 Mode TUN/TAP

Dans le mode TUN/TAP, QEmu crée une carte réseau virtuelle directement sur le système hôte, par l'intermédiaire de laquelle il aura accès au réseau. Cette approche diffère du mode utilisateur, qui s'appuie simplement sur la configuration réseau existante de l'hôte, sans ajouter de matériel.

Ce mode est utilisable facilement sur les hôtes Linux, mais pour un hôte Windows, il est nécessaire d'installer un produit pouvant créer un adaptateur TAP. OpenVPN (http://openvpn.net), par exemple, peut être utilisé à cette fin. Une procédure de configuration, en anglais, existe ici : http://www.h7.dion.ne.jp/~qemu-win/TapWin32-en.html#vlan.

**** A compléter ****

5.2.1.2 VLAN

Le VLAN permet de connecter plusieurs machines virtuelles entre elles. QEmu permet de construire ce réseau de plusieurs manières différentes. Il peut être limité aux instances de QEmu, ou ouvert sur l'Internet, par l'intermédiaire du réseau user mode ou TUN/TAP.

Note : Cette option ne semble pas fonctionner correctement avec un hôte Windows pour le moment, l'option `connect` n'étant pas reconnue... Un patch est disponible ici : http://www.h7.dion.ne.jp/~qemu-win/, mais il n'est pas certain qu'il s'applique correctement sur les derniers sources CVS.

Quoi qu'il en soit, le schéma ci-dessous illustre les combinaisons possibles pour construire un VLAN avec QEmu. Il est bien sûr possible de n'en implémenter qu'une partie.

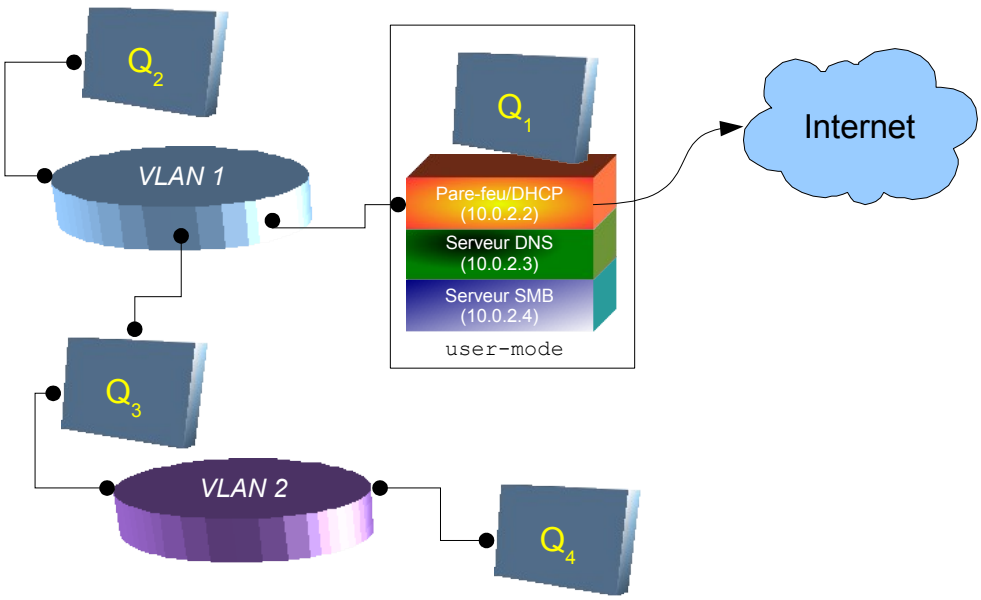


Illustration 5: VLAN - Toutes les combinaisons

- Q_n représente une instance de QEmu
- L'instance Q_1 est configurée pour utiliser le réseau en mode utilisateur, permettant l'accès à Internet.

– Les instances Q_3 et Q_4 sont sur un VLAN différent.

– Q_3 possède deux cartes réseaux, chacune sur un VLAN différent.

– Lorsqu'il n'est pas précisé, VLAN=0 par défaut.

Les options de ligne de commande qui permettent de configurer le VLAN sont les suivantes :

```
-net user[,vlan=n][,hostname=host]
-net tap[,vlan=n],ifname=name
-net socket[,vlan=n][,fd=h][,listen=[host]:port][,connect=host:port]
-net socket[,vlan=n][,fd=h][,mcast=maddr:port]
```

En combinant ces options, il est possible de réaliser tout ou partie du VLAN décrit ci-dessus.

Les points à prendre en considération lorsqu'on construit un VLAN sont les suivants :

- chaque carte réseau virtuelle doit avoir une **adresse MAC différente** ;
- chaque machine virtuelle doit se voir attribuer une adresse IP différente, dans la plage autorisée par le masque de sous-réseau (255.255.255.0) ;
- les noms des machines (dans le SE cible) doivent être différents.

Cette option n'étant pas utilisable pour le moment sous Windows, nous nous bornerons à l'aborder sur le plan théorique. Voici, dans le principe, les lignes de commande à taper pour obtenir la configuration ci-dessus :

**** A compléter ****

5.2.1.3 Autres options réseau

Autres options réseau de QEmu.

`-redir [tcp|udp]:host-port:[guest-host]:guest-port` : permet de rediriger des ports TCP ou UDP de l'hôte vers la machine virtuelle. Nécessite l'emploi de `-net user` (option par défaut).

`[tcp|udp]`, facultatif, indique si le port redirigé est un port TCP ou UDP

`host-port` : numéro du port du système hôte qui doit être redirigé.

`[guest-host]`, facultatif, est l'adresse IP du système cible sur le VLAN QEmu (10.0.2.15 par défaut).

`guest-port` : port du système cible vers lequel le port hôte est redirigé.

Reportez vous au paragraphe 5.2.5, page 29 pour un exemple de redirection. Pour rediriger d'autres ports, ajoutez autant d'options `-redir` que nécessaire.

5.2.2 Partage de fichiers avec l'hôte

5.2.2.1 La disquette

C'est le moyen le plus simple pour échanger des fichiers entre l'hôte et la machine virtuelle. Il est reconnu par tous les SE. L'échange est possible en lecture et en écriture dans les deux sens (***hôte <---> machine virtuelle***).

Inconvénients : il n'est pas très rapide, et sa capacité est très limitée.

La commande `change fda //./a:` du moniteur permet d'insérer une disquette dans la machine virtuelle.

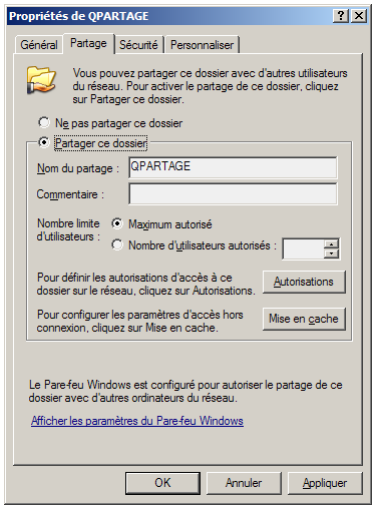
La commande `eject fda` retire la disquette du lecteur de la machine virtuelle.

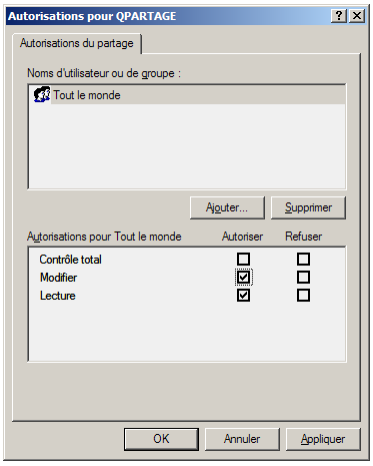
5.2.2.2 Partage Microsoft

Sans doute le moyen le plus souple et le plus efficace lorsque l'hôte et la cible sont des SE Microsoft. Ce mode permet de partager des fichiers en lecture et en écriture dans les deux sens (***hôte <---> machine virtuelle***). Aucune option n'est nécessaire sur la ligne de commande de QEmu, sinon que le support réseau doit être activé.

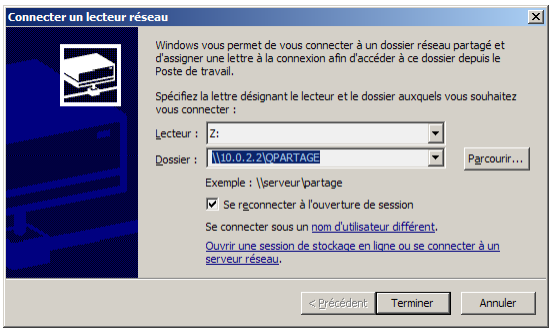
– Créez un dossier sur le disque dur de l'hôte : C:\QEMU\QPARTAGE, par exemple.

– Faites un clic-droit sur ce dossier, puis cliquez sur **Partage et sécurité**. Donnez un nom au partage, puis cliquez sur le bouton Autorisations. Attribuez les droits de **Lecture** et **Modifier** au groupe **Tout le monde**.


Propriétés de QPARTAGE
Général
Partage
Sécurité
Personnaliser
Vous pouvez partager ce dossier avec d'autres utilisateurs du réseau. Pour activer le partage de ce dossier, cliquez sur Partager ce dossier.
Ne pas partager ce dossier
Partager ce dossier
Nom du partage :
QPARTAGE
Commentaire :
Nombre limite d'utilisateurs :
Maximum autorisé
Nombre d'utilisateurs autorisés :
Pour définir les autorisations d'accès à ce dossier sur le réseau, cliquez sur Autorisations.
Autorisations
Pour configurer les paramètres d'accès hors connexion, cliquez sur Mise en cache.
Mise en cache
Le Pare-feu Windows est configuré pour autoriser le partage de ce dossier avec d'autres ordinateurs du réseau.
Afficher les paramètres du Pare-feu Windows
OK
Annuler
Appliquer



– Passez ensuite dans le SE cible, ouvrez un explorateur Windows (si vous avez installé Windows dans QEmu), cliquez sur Outils, Connecter un lecteur réseau. Choisissez une lettre pour le lecteur, dans la zone Dossier, entrez \\10.0.2.2\<NomDuPartage>, cochez la case Se reconnecter à l'ouverture de session.


Connecter un lecteur réseau
Windows vous permet de vous connecter à un dossier réseau partagé et d'assigner une lettre à la connexion afin d'accéder à ce dossier depuis le Poste de travail.
Spécifiez la lettre désignant le lecteur et le dossier auxquels vous souhaitez vous connecter :
Lecteur :
Z:
Dossier :
\\10.0.2.2\QPARTAGE
Parcourir...
Exemple : \\serveur\partage
Se reconnecter à l'ouverture de session
Se connecter sous un nom d'utilisateur différent.
Ouvrir une session de stockage en ligne ou se connecter à un serveur réseau.
< Précédent
Terminer
Annuler

Vous pouvez maintenant partager des fichiers.

Si le SE cible est Windows 9x, la procédure de connexion sous QEmu est légèrement différente (la création du partage sur l'hôte reste identique). **Dans le SE cible** :

– Commencez par modifier le fichier C:\Windows\hosts. En principe, ce fichier ne contient qu'une seule ligne, de la forme : `127.0.0.1 localhost`.

  Ajoutez une ligne similaire à ce fichier, contenant : `nnn.nnn.nnn.nnn` `<NomHOTE>`. Pour obtenir ces deux informations, tapez, sur l'hôte, une commande `ipconfig /all`. Vous trouverez dans les lignes **Nom de l'hôte** et **Adresse IP** les informations nécessaires. Il s'agit bien des nom et adresse IP de l'hôte qu'il faut inscrire dans le fichier hosts du SE cible. Vous pouvez enregistrer et fermer le fichier hosts.

– La connexion du lecteur réseau se fait ensuite de la même manière que ci-dessus.

Dans un SE cible d'origine non-Microsoft, il existe souvent une procédure similaire. `smbclient` doit être installé lorsque Linux est le SE cible pour reconnaître les partages Microsoft. D'autres SE peuvent avoir des modules équivalents.

Remarque : ce partage n'est possible que si le support réseau (user mode ou TUN/TAP) est configuré.

5.2.2.3 Partage de répertoire hôte

Cette option permet des transferts ***hôte ---> machine virtuelle***. Le répertoire désigné sur la ligne de commande de QEmu apparaît au SE cible comme un nouveau lecteur de disques. Tout le contenu existant de ce répertoire est visible. Il est possible d'écrire sur ce disque, mais les modifications ne sont pas répercutées vers le dossier de l'hôte, et ne sont pas conservées. Après un redémarrage de QEmu, toutes les modifications sont perdues.

L'option à ajouter à la ligne de commande est :

`-hdd fat:c:\temp` par exemple, pour monter ce dossier comme nouveau disque dans QEmu. Dans ce cas, ce sera le disque E:. Le nom de ce lecteur sera **QEMU VVFAT**. Un répertoire peut également être monté en tant que disquette en utilisant `-fda fat:floppy:c:\temp`.

L'option `-fda fat:floppy:rw:c:\temp` permet de valider l'écriture dans le dossier de l'hôte, mais cette variante, utilisable uniquement avec le paramètre `:floppy:` n'est pas encore stabilisée : à utiliser avec précautions.

5.2.2.4 Partage par TFTP

QEmu permet d'accéder à un dossier de l'hôte par l'intermédiaire du protocole TFPT (Trivial File Transfer Protocol), version simplifiée de FTP. Cette possibilité suppose l'emploi de l'option `-net user` (option par défaut) sur la ligne de commande de QEmu.

Si le SE cible n'a pas de client TFTP, il faut en installer un. Windows 2000, par exemple, possède un client TFTP intégré.

Pour utiliser le transfert par TFTP, il faut indiquer à QEmu le répertoire dans lequel il pourra lire les fichiers. L'écriture n'est pas possible. Le transfert est limité au sens ***hôte ---> machine virtuelle***, un seul fichier à la fois (les caractères génériques - *, ? - ne sont pas autorisés). On ajoutera donc à la ligne de commande l'option `-tftp /Temp` si on veut partager le répertoire **\Temp** de l'hôte. Ce répertoire devra être situé sur le même disque que le fichier qemu.exe.

Dans la machine virtuelle, il sera alors possible de transférer un fichier :

```
C:\>TFTP -i 10.0.2.2 get /temp/essai.txt \temp\essait.txt
```

où :
`/temp/essai.txt` est le fichier à copier depuis l'hôte;
`\temp\essai.txt` est la destination dans le client. Ce paramètre est facultatif. Il peut se résumer à un nom de fichier.

Bien entendu, le dossier déclaré pour le transfert TFTP ne peut être changé que lors d'un redémarrage de QEmu.

5.2.2.5 Partage par SMB

Ne semble pas fonctionner actuellement, sur un hôte Windows en tout cas...

Le partage SMB ressemble fortement au partage Microsoft (ce qui est normal puisque SMB est le protocole Microsoft pour le partage de fichiers en réseau), mis à part que le nom du dossier partagé est figé lors du démarrage de QEmu. La ligne de commande de QEmu doit être complétée par `-smb /Temp` si l'on veut partager le répertoire C:\Temp.

Il faut ensuite, dans l'hôte, ajouter au fichier lmhosts (C:\WINDOWS\LMHOSTS pour Windows 9x, C:\WINDOWS\SYSTEM32\DRIVERS\ETC\LMHOSTS pour Windows 2000-XP) la ligne :

```
10.0.2.4     smbserver
```

Le dossier partagé est ensuite accessible depuis le SE cible par la syntaxe \\smbserver\qemu. Ce nom peut être utilisé pour connecter un lecteur réseau.

Si le SE hôte n'est pas un SE Microsoft, il faudra y installer un serveur SMB (samba par exemple pour Linux)

5.2.3 Support USB

L'option `-usb` de la ligne de commande active le contrôleur USB de la machine virtuelle. Si cette option est omise, la machine virtuelle démarre sans contrôleur USB. Dans sa version actuelle pour Windows, QEmu ne peut pas utiliser les périphériques USB physiques. La version pour Linux, par contre, le permet.

Pour '*brancher*' un périphérique USB lors du démarrage de QEmu, utilisez l'option `-usbdevice` sur la ligne de commande. Voyez l'option `usb_add` du moniteur pour plus d'informations (paragraphe 5.3.5, page 33).

5.2.4 Support Audio

Les options de cette section permettent d'installer une ou plusieurs cartes sonores dans la machine virtuelle. `-audio-help` permet d'en connaître toutes les variantes :

```
C:\QEMU>qemu -audio-help
```

```
Audio options:
  QEMU_AUDIO_DAC_FIXED_SETTINGS: boolean, default = 1
    Use fixed settings for host DAC
  QEMU_AUDIO_DAC_FIXED_FREQ: integer, default = 44100
    Frequency for fixed host DAC
  QEMU_AUDIO_DAC_FIXED_FMT: format, default = S16, (one of: U8 S8 U16 S16)
    Format for fixed host DAC
  QEMU_AUDIO_DAC_FIXED_CHANNELS: integer, default = 2
    Number of channels for fixed DAC (1 - mono, 2 - stereo)
  QEMU_AUDIO_DAC_VOICES: integer, default = 1
    Number of voices for DAC
  QEMU_AUDIO_ADC_FIXED_SETTINGS: boolean, default = 1
    Use fixed settings for host ADC
  QEMU_AUDIO_ADC_FIXED_FREQ: integer, default = 44100
    Frequency for fixed host ADC
  QEMU_AUDIO_ADC_FIXED_FMT: format, default = S16, (one of: U8 S8 U16 S16)
    Format for fixed host ADC
  QEMU_AUDIO_ADC_FIXED_CHANNELS: integer, default = 2
    Number of channels for fixed ADC (1 - mono, 2 - stereo)
  QEMU_AUDIO_ADC_VOICES: integer, default = 1
    Number of voices for ADC
  QEMU_AUDIO_TIMER_PERIOD: integer, default = 0
    Timer period in HZ (0 - use lowest possible)
  QEMU_AUDIO_PLIVE: boolean, default = 0
    (undocumented)
  QEMU_AUDIO_LOG_TO_MONITOR: boolean, default = 0
    print logging messages to montior instead of stderr

Available drivers:
Name: sdl
Description: SDL http://www.libsdl.org
One playback voice
Does not support capture
Options:
  QEMU_SDL_SAMPLES: integer, default = 1024
    Size of SDL buffer in samples

Name: none
Description: Timer based audio emulation
Theoretically supports many playback voices
Theoretically supports many capture voices
No options

Name: wav
Description: WAV renderer http://wikipedia.org/wiki/WAV
One playback voice
Does not support capture
Options:
  QEMU_WAV_FREQUENCY: integer, default = 44100
    Frequency
  QEMU_WAV_FORMAT: format, default = S16, (one of: U8 S8 U16 S16)
    Format
  QEMU_WAV_DAC_FIXED_CHANNELS: integer, default = 2
    Number of channels (1 - mono, 2 - stereo)
  QEMU_WAV_PATH: string, default = qemu.wav
    Path to wave file

Options are settable through environment variables.
Example:
  set QEMU_AUDIO_DRV=wav
  set QEMU_WAV_PATH=c:\tune.wav
```

```
qemu ...
```

On peut voir que QEmu permet un paramétrage très pointu des périphériques audio. Sans entrer dans le détail de ces options, il est possible d'activer l'émulation sonore simplement en choisissant le ou les périphériques adéquats. En fonction des options de compilation, certaines émulations audio peuvent être disponibles ou non. Tapez la commande suivante pour en prendre connaissance.

```
C:\QEMU>qemu -soundhw ?
Valid sound card names (comma separated):
pcspk       PC speaker
sb16        Creative Sound Blaster 16
es1370      ENSONIQ AudioPCI ES1370

-soundhw all will enable all of the above
```

Dans le cas de l'exemple ci-dessus, trois périphériques sonores sont disponibles : le haut-parleur du PC, une SoundBlaster 16 et une Ensoniq ES1370. La carte compatible AdLib n'est disponible que si l'option `-enable-adlib` a été ajoutée sur la ligne de commande de `./configure` (paragraphe 3.2.4, page 9), avant la compilation de QEmu.

Pour *installer* une SB16 et une ES1370, il faut fournir le paramètre suivant à la ligne de commande : `-soundhw sb16,es1370`. Pour installer automatiquement toutes les cartes sonores disponibles, utilisez l'option `-soundhw all`.

5.2.5 Support VNC

VNC (http://fr.wikipedia.org/wiki/VNC) est un protocole permettant de se connecter à un ordinateur distant, pour en prendre le contrôle comme si on était assis devant. QEmu intègre un serveur VNC qui peut être activé avec l'option `-vnc n`. Dans ce cas, QEmu démarre sans fenêtre visible (on ne voit rien directement à l'écran), mais on peut s'y connecter avec n'importe quel client VNC (UltraVNC : http://ultravnc.sourceforge.net/, RealVNC : http://www.realvnc.com/ par exemple, mais il en existe bien d'autres). `n` est le numéro d'écran sur lequel le client devra se connecter.

Lancez votre client VNC, puis connectez vous sur : `127.0.0.1:n` ou `localhost:n`. Il sera probablement nécessaire d'autoriser l'option *loopback connections* du client, sinon VNC refusera de se connecter au poste sur lequel il s'exécute.

En combinant cette option avec l'option `-redir`, il est possible de se connecter sur une instance QEmu depuis un autre ordinateur du réseau (redirection du port 5900, communément utilisé par VNC). Voici comment cela est possible :

Sur un premier ordinateur, que nous appellerons PC01, lancer QEmu avec une ligne de commande semblable à celle-ci :

```
qemu.exe ..... -usb -usbdevice tablet -redir tcp:5890::5900 -vnc 1 -k fr
```

– L'option `-redir` permet de rediriger le port 5890 (le numéro 5890 est arbitraire) de l'hôte (PC01) vers le port 5900 de la machine virtuelle (le port 5900 est le port par défaut utilisé par VNC).

– L'option `-vnc 1` indique au serveur VNC de QEmu que les clients se connecteront sur l'écran n° 1.

A partir du PC02, le client VNC (viewer) se connectera en utilisant la syntaxe : `PC01:1:5890`. Dans les options du client, il faudra prendre soin de choisir un encodage Hextile, et une profondeur de 256 couleurs. Suivant le client VNC utilisé (UltraVNC, RealVNC, TightVNC, etc...), il faudra parfois jouer sur d'autres options d'encodage pour obtenir une stabilité maximale de la connexion.

Remarque : l'utilisation de l'option `-vnc` nécessite l'option `-k` (paragraphe 5.2.6, page 30) pour imposer la langue du clavier.

5.2.6 Autres options

Voici encore quelques options qui n'entrent pas dans les catégories précédentes :

`-boot [a|c|d]` : permet de choisir le périphérique de démarrage de la machine virtuelle. `c` est la valeur par défaut lorsqu'aucune option `boot` n'est précisée.

`-snapshot` : cette option s'applique aux images disques. Lorsqu'elle est utilisée, les écritures ne sont pas faites dans

l'image, mais dans un fichier temporaire. Lorsqu'on quitte QEmu, toutes les écritures faites sur les disques durs pendant la session sont ignorées. Cette option est équivalente à l'utilisation d'une image de base automatique et temporaire (voir qemu-img). Une commande du moniteur permet toutefois de valider ces écritures en les intégrant dans le fichier image.

`-m nnn` : permet d'allouer `nnn` Mo de RAM à la machine virtuelle. La valeur par défaut est de 128 Mo. Ajustez cette valeur en fonction des besoins du SE cible.

`-smp n` : permet de simuler une machine à plusieurs processeurs. n peut aller de 1 à 255, la valeur par défaut étant 1.

`-win2k-hack` : cette option peut se révéler nécessaire lorsqu'on installe Windows 2000 en tant que SE cible. L'installation de W2K se met parfois en boucle, remplissant complètement l'image disque. Ce paramètre permet d'éviter cette erreur, mais il ralentit l'émulateur. Ne l'utilisez pas en fonctionnement normal, mais seulement pendant l'installation de Windows 2000.

`-S` : cette option permet de figer la machine virtuelle dès le chargement de QEmu. Cela peut vous laisser le temps de changer l'affinité du processus avant de relancer l'exécution normale (commande `cont` ou `c` du moniteur).

`-std-vga` permet de remplacer la carte Cirrus Logic GD-5446 (carte par défaut) par une carte VGA VESA standard. Peut être utilise si le SE cible ne reconnaît pas correctement la carte par défaut.

`-no-acpi` désactive le support ACPI (http://fr.wikipedia.org/wiki/ACPI) si le SE cible ne réagit pas correctement à cette interface.

`-loadvm <fichier>` : jusqu'à la version 0.8.1, le moniteur, avec sa commande `savevm` permettait de sauvegarder l'état complet d'une machine virtuelle avant d'arrêter QEmu (un peu l'équivalent de la mise en hibernation de Windows, ou toute la RAM est sauvegardée dans un fichier). Cette option permet de recharger cet état au démarrage du programme. <fichier> fait référence au nom donné lors de la sauvegarde de l'état.

Depuis la version 0.8.2, le fonctionnement de cette commande a changé. Voyez le paragraphe 5.3.7, page 33 pour plus de précisions.

`-k <langue>` : permet de forcer la disposition du clavier. Cette option est nécessaire lorsqu'on utilise l'option `-vnc` (paragraphe 5.2.5, page 29), sinon QEmu émule un clavier américain. `<langue>` peut être :

```
ar  de-ch  es  fo     fr-ca  hu  ja  mk     no  pt-br  sv
da  en-gb  et  fr     fr-ch  is  lt  nl     pl  ru     th
de  en-us  fi  fr-be  hr     it  lv  nl-be  pt  sl     tr
```

Les fichiers de disposition du clavier se trouvent dans C:\MSYS\\home\<NomUtilisateur>\qemu\keymaps. Copiez ce dossier dans le le dossier C:\QEMU\BIOS afin que QEmu puisse trouver les définitions de clavier.

- `no-quit` : cette option rend inopérante la croix de fermeture de la fenêtre. Il ne reste donc plus que deux possibilités pour quitter QEmu : l'arrêt normal par le SE cible, ou alors la commande `q` (`quit`) du moniteur. Si, pour une raison ou une autre, il n'est pas possible de passer en mode moniteur, il faudra en passer par le gestionnaire des tâches de Windows.
- `no-reboot` : lors de leur installation, la plupart des SE vont demander un ou plusieurs redémarrages de la machine virtuelle, ce qui pose un problème lorsque le démarrage à partir du CD ne peut être contourné. En effet, l'option `-boot` de la ligne de commande ne peut être changée sans arrêter QEmu et le relancer. L'installation du SE cible risque donc de se mettre en boucle, puisqu'il n'est pas possible de dire à QEmu de démarrer à partir de C:. L'éjection du CD (virtuel) ne suffit par, car QEmu voudra quand même démarrer à partir du lecteur de CD.

  L'option `-no-reboot` indique à QEmu de traiter une demande de redémarrage venant du SE cible comme un arrêt de la machine virtuelle. Il suffit alors de relancer QEmu, sans option `-boot` pour terminer l'installation.

  Note : Windows 2000 et supérieur ne nécessitent pas l'emploi de cette option car ils affichent le message « Appuyez sur une touche pour démarrer à partir du CD ». Il suffit donc de ne pas toucher le clavier pour démarrer à partir du disque dur. Si le SE que vous installez propose le même mécanisme, ou permet de choisir le périphérique de démarrage, vous n'aurez pas besoin de cette option.
- `-option-rom` : permet de charger une ROM dans l'espace d'adressage réservé aux extensions. Le contenu de cette ROM sera détecté par le BIOS et exécuté lors du démarrage du PC virtuel.

5.3 Le moniteur

Le moniteur permet de modifier certains paramètres de la machine virtuelle et d'en inspecter l'état. Certaines de ses commandes sont plutôt destinées aux développeurs ; nous ne les aborderons pas, pour nous concentrer sur les plus utiles.

L'entrée dans le mode moniteur se fait en appuyant sur les touches **Ctrl-Alt-2**. Pour revenir à l'écran principal de QEmu, il faut appuyer sur les touches **Ctrl-Alt-1**.

Remarque : lorsqu'on entre dans le moniteur, la première touche tapée au clavier n'est pas prise en compte... Suivant le SE cible, lorsqu'on revient à l'écran principal, un ou plusieurs caractères parasites peuvent êtres transmis (souvent le **1** ou **&**).

En tapant `help`, ou `?` dans le moniteur, on obtient la liste des commandes disponibles.

```
Help|?                  show the help
commit                  commit changes to the disk images (if -snapshot is used)
info subcommand         show various information about the system state
q|quit                  quit the emulator
eject [-f] device       eject a removable media (use -f to force it)
change device filename change a removable media
screendump filename     save screen into PPM image 'filename'
log item1[,...]         activate logging of the specified items to '/tmp/qemu.log'
savevm [tag|id]         save a VM snapshot. If no tag or id are provided, a new
snapshot is created
loadvm tag|id           restore a VM snapshot from its tag or id
delvm tag|id            delete a VM snapshot from its tag or id
stop                    stop emulation
c|cont                  resume emulation
gdbserver [port]        start gdbserver session (default port=1234)
x /fmt addr             virtual memory dump starting at 'addr'
xp /fmt addr            physical memory dump starting at 'addr'
p|print /fmt expr print expression value (use $reg for CPU register access)
i /fmt addr             I/O port read
sendkey keys            send keys to the VM (e.g. 'sendkey ctrl-alt-f1')
system_reset            reset the system
system_powerdown        send system power down event
sum addr size           compute the checksum of a memory region
usb_add device          add USB device (e.g. 'host:bus.addr' or
'host:vendor_id:product_id')
usb_del device          remove USB device 'bus.addr
cpu index               set the default CPU
```

Certaines commandes, comme la commande `info`, ont encore des sous-commandes.

5.3.1 La commande info

La commande `info` admet les sous-commandes suivantes :

`version` Affiche le numéro de version de QEmu

`network` Affiche des informations sur le réseau dans QEmu.

```
(qemu) info network
VLAN 0 devices:
  user redirector
  ne2000 pci macaddr=52:54:00:12:34:56
```

`block` Affiche des informations sur les disques virtuels

```
(qemu) info block
  cdrom: type=cdrom removable=1 locked=0 [not inserted]
  hda: type=hd removable=0 file=<NomImage>
backing_file=<NomImageBase> ro=0 drv=qcow2
  hdb: type=hd removable=0 file=<NomImage> ro=0 drv=qcow2
  fda: type=floppy removable=1 locked=0 file=//./A: ro=0 drv=raw
```

`registers` Affiche les registres du processeur virtuel.

`cpus` Affiche des informations sur chaque processeur virtuel.

`history` Affiche l'historique des commandes tapées dans le moniteur.

`irq` Affiche des statistiques sur les requêtes IRQ (si disponible).

`pic` Affiche des informations sur le PIC i8259.

`pci` Affiche des informations sur le bus PCI de la machine virtuelle.

`tlb` Affiche des informations sur les correspondances mémoire virtuelle vers physique.

`mem` Informations sur la mémoire virtuelle.

`jit` Affiche les statistiques du compilateur dynamique.

`kqemu` Affiche l'état du module accélérateur (kqemu) :

```
(qemu) info kqemu
kqemu support: enabled for user and kernel code
```

`usb` Liste les périphériques USB de la machine virtuelle :

```
(qemu) info usb
  Device 0.2, Speed 12 Mb/s, Product QEMU USB Tablet
```

`usbhost` Liste les périphériques USB de l'hôte. Ne fonctionne que si un filtre USB est installé sur l'hôte (Windows) et nécessite également une version patchée de QEmu.

`snapshot` affiche des informations sur les instantanés enregistrés dans les images diques.

5.3.2 Éjecter/Changer un CD ou une disquette

Nous l'avons déjà vu auparavant, changer un périphérique de stockage virtuel se fait avec la commande `change`.

`change device filename`.

> `device` représente le lecteur virtuel concerné : `fda` ou `fdb` pour les lecteurs de disquettes, `cdrom` pour le lecteur de CD. Les disques durs ne sont pas amovibles...
>
> `filename` est le chemin d'accès complet (nom du fichier inclus) du fichier image de disquette ou de CD/DVD. L'accès à un périphérique physique est possible avec la syntaxe \\.\X: ou //./X: (X représentant la lettre du lecteur physique).

La commande `eject [-f] device` permet d'éjecter le média du lecteur virtuel. `device` peut prendre les mêmes valeurs que pour la commande `change`. L'option `-f` permet de forcer l'éjection du média, même si le SE cible verrouille le lecteur (Linux, par exemple).

5.3.3 Redémarrer la machine virtuelle

De même que l'hôte possède un bouton RESET, la machine virtuelle peut être redémarrée à l'aide de la commande `system_reset`. Cette commande n'a pas de paramètre.

5.3.4 Suspendre/Éteindre QEmu

La machine virtuelle peut être suspendue avec la commande `stop`. Vivement recommandé avant de sauvegarder l'état de la machine virtuelle, par exemple. `c` ou `cont` permet de reprendre l'exécution normale.

`q` ou `quit` permet d'éteindre sauvagement la machine virtuelle. Ça revient à débrancher la prise secteur d'un hôte... Dans la mesure du possible, il est préférable d'arrêter QEmu par l'intermédiaire du SE cible.

5.3.5 Commandes USB

QEmu reconnaît les valeurs suivantes pour le paramètre `device` : `mouse`, `tablet` et `disk`. Ces mêmes valeurs peuvent être utilisées sur la ligne de commande de QEmu avec l'option `-usbdevice`. La ligne de commande de

QEmu semble n'accepter qu'un seul paramètre `-usbdevice`. Les autres périphériques à connecter devront l'être par l'intermédiaire du moniteur.

La commande `usb_add device` permet de *brancher* un périphérique USB virtuel.

Pour brancher une souris USB à la machine virtuelle, tapez : `usb_add mouse`. Cette souris remplacera la souris PS/2 par défaut.

Pour brancher une tablette USB à la machine virtuelle, tapez : `usb_add tablet`. La tablette USB permet surtout de s'affranchir de la capture du pointeur de la souris. Elle remplace la souris PS/2.

Il est aussi possible de monter un fichier image comme disque USB, avec l'option `disk:`. La commande `usb_add disk:C:\QEMU\IMAGES\<Image.img>` provoquera l'apparition d'un nouveau disque amovible USB. Ce disque pourra être déconnecté (`usb_del x.y`) et reconnecté comme n'importe quel périphérique USB (`usb_add`). Ce périphérique est accessible en lecture et en écriture.

```
(qemu) info usb
  Device 0.2, Speed 12 Mb/s, Product QEMU USB MSD(C:\QEMU\IMAGES\<Image.img>)
```

La commande `usb_del bus.adresse` permet de retirer un périphérique. `bus.adresse` vous sera fourni par la commande `info usb` (voir un peu plus haut).

5.3.6 Envoyer des séquences de touches

La commande `sendkey` permet d'envoyer des séquences de touches à la machine virtuelle. Plusieurs touches peuvent être combinée en les séparant par un tiret : `sendkey ctrl-alt-delete` permet d'envoyer Control-Alt-Suppr à la machine virtuelle, séquence normalement interceptée par Windows si elle est tapée sur le clavier de l'hôte. `sendkey 0x1d-0x38-0xd3` donnerait le même résultat.

Attention toutefois si vous envoyez des codes de caractères imprimables (lettres, chiffres, etc...) : ils sont interprétés comme venant d'un clavier américain (0x1e affichera q dans le SE cible). De plus, des caractères parasites sont insérés... Cette commande est surtout utile pour les séquences de touches qui sont interceptées par l'hôte. Vous trouverez en annexe la liste des codes reconnus par la commande (paragraphe 9.1, page 38).

5.3.7 Sauver/Charger la machine virtuelle

A partir de la version 0.8.2, la commande `savevm` change : les instantanés ne sont plus enregistrés dans un fichier séparé, mais directement dans une image disque (en général, la première correspondant aux critères ci-dessous), qui doit obligatoirement être au format qcow2 (le format qcow ne prend pas en charge cette fonctionnalité). Ceci implique d'avoir au moins une image disque au **format qcow2**, qui ne soit **pas amovible** et accessible en **écriture**.

L'intérêt de cette approche est de pouvoir suivre les modifications apportées aux disques virtuels, ce qui n'était pas envisageable lorsque l'état était enregistré dans un fichier séparé.

Un instantané mémorise l'état complet d'une machine virtuelle : état du processeur, mémoire vive, état des périphériques et modifications (écritures) faites sur les disques virtuels. Il est alors possible de *photographier* la machine virtuelle et de revenir a un état précédent : le PC virtuel possède une option Edition/Annuler !

Pour créer un instantané, utilisez la commande `savevm [tag|id]`. `tag` représente un nom que vous attribuez à la sauvegarde. `id` est un numéro que QEmu attribue à la sauvegarde. Cette information est facultative.

Si `tag` ou `id` est fourni, et qu'un instantané porte déjà cet identifiant, il est écrasé. Sinon, un nouvel instantané est créé.

Les commandes `loadvm tag|id` et `delvm tag|id` sont les compléments évidents de la commande `savevm`, permettant de rappeler un état enregistré, ou de le supprimer.

La commande `info snapshots` permet de connaître la liste des instantanés :

```
(qemu) info snapshots
Snapshot devices: hda
Snapshot list (from hda):
ID        TAG                 VM SIZE                DATE       VM CLOCK
```

```
1         SAVE1                   45M aaaa-mm-jj hh:mm:ss   hh:mm:ss.mmm
```

Remarque : il ne faut pas confondre les *instantanés* avec la notion *d'image de base*. Un instantané mémorise l'état complet de la machine virtuelle, alors qu'une image disque basée sur une autre n'enregistre que les modifications de ce disque virtuel.

5.3.8 Autres commandes

Les commandes restantes sont plutôt utilisées pour le développement. Elles permettent d'examiner la mémoire ou les ports d'entrées/sorties et ne sont pas très importantes pour une utilisation normale.

On peut citer rapidement la commande `commit`, qui est utile si QEmu a été démarré avec l'option `snapshot`. Cette option transfère toutes les écritures qui ont été faites sur l'image de disque temporaire vers l'image de base.

6 Utilitaires divers

– Compression/décompression :

  La plupart des fichiers que vous téléchargerez sont comprimés, surtout s'il s'agit d'une image disque de plusieurs centaines de Mo, voire quelques Go.

  Étant fortement lié au monde GNU/Linux et au logiciel libre, les fichiers proposés par ces projets sont souvent au format gzip, très répandu dans la communauté Open Source. Si votre logiciel de compression habituel ne connaît pas ce format, vous pouvez utiliser l'un de ceux-ci, qui ont en plus l'avantage d'être gratuits :

  7zip : http://www.7zip.org – licence LGPL – 63 langues dont le français – (formats **écrits**/lus : **7z, ZIP, GZIP, BZIP2, TAR, RAR**, CAB, ISO, ARJ, LZH, CHM, Z, CPIO, RPM, DEB, NSIS).

  alzip : http://www.altools.net

  filzip : http://www.filzip.com/en/index.html

  izarc : http://www.florida.plus.com/izarc/

  quickzip : http://www.quickzip.org

  zipgenius : http://www.zipgenius.it

  etc...

– Images CD et disquettes :

  Pour créer une image ISO d'un CD ou DVD, vous pouvez utiliser votre logiciel de gravage (Nero, EasyCD Creator, etc...). Ils sont souvent pourvus d'une option permettant de créer une image à partir d'un CD/DVD.

  A défaut, vous pouvez par exemple utiliser IsoBuster (http://www.smart-projects.net/fr/isobusterdownloads.php).

  Reportez-vous au mode d'emploi du logiciel pour la création d'une image.

– imagecfg :

  imagecfg est un utilitaire Microsoft qui permet de modifier l'en-tête d'un fichier exécutable. Il peut se trouver sur le CD de Windows NT 4, mais aussi très facilement sur le Web. Pour QEmu, il nous servira surtout à forcer l'exécution sur un seul coeur.

  Attention : les modifications faites par imagecfg ne sont pas réversibles. Pensez à sauvegarder le fichier exécutable avant de le modifier.

  Téléchargez et placez imagecfg.exe dans C:\WINDOWS\SYSTEM32 si vous voulez l'utiliser avec d'autres fichiers exe. Si vous ne prévoyez de l'utiliser qu'avec QEmu, vous pouvez le mettre dans C:\QEMU.

```
C:\QEMU>imagecfg -a 0x2 qemu.exe
qemu.exe contains no configuration information
qemu.exe contains a Subsystem Version of 4.0
qemu.exe updated with the following configuration information:
    Process Affinity Mask: 00000002
```

Comme vous pouvez le voir sur l'exemple ci-dessus, c'est l'option `-a` qui nous intéresse. Le numéro du processeur (ou coeur) à affecter au processus qemu.exe doit être fourni en hexadécimal : `0x1` pour le coeur n°1, `0x2` pour le coeur n° 2, etc...

Qemu.exe s'exécutera alors sur un seul coeur et sa stabilité en sera grandement améliorée.

Note : cette opération doit être faite après chaque nouvelle compilation de qemu.exe.

7 Liens

http://qemu.org
Le site officiel de QEmu. Vous y trouverez les sources de la dernière version stable, l'accélérateur, les documentations, des liens...

http://qemu.dad-answers.com
Le forum des utilisateurs. Vous pouvez également me laisser un message ici : http://qemu.dad-answers.com/viewtopic.php?t=1852.

http://bochs.sourceforge.net
Un émulateur de plate-forme Intel x86.

http://fr.wikipedia.org/wiki/Qemu
QEmu sur Wikipedia.

8 Copies d'écrans

Illustration 6: Windows 2000 dans QEmu

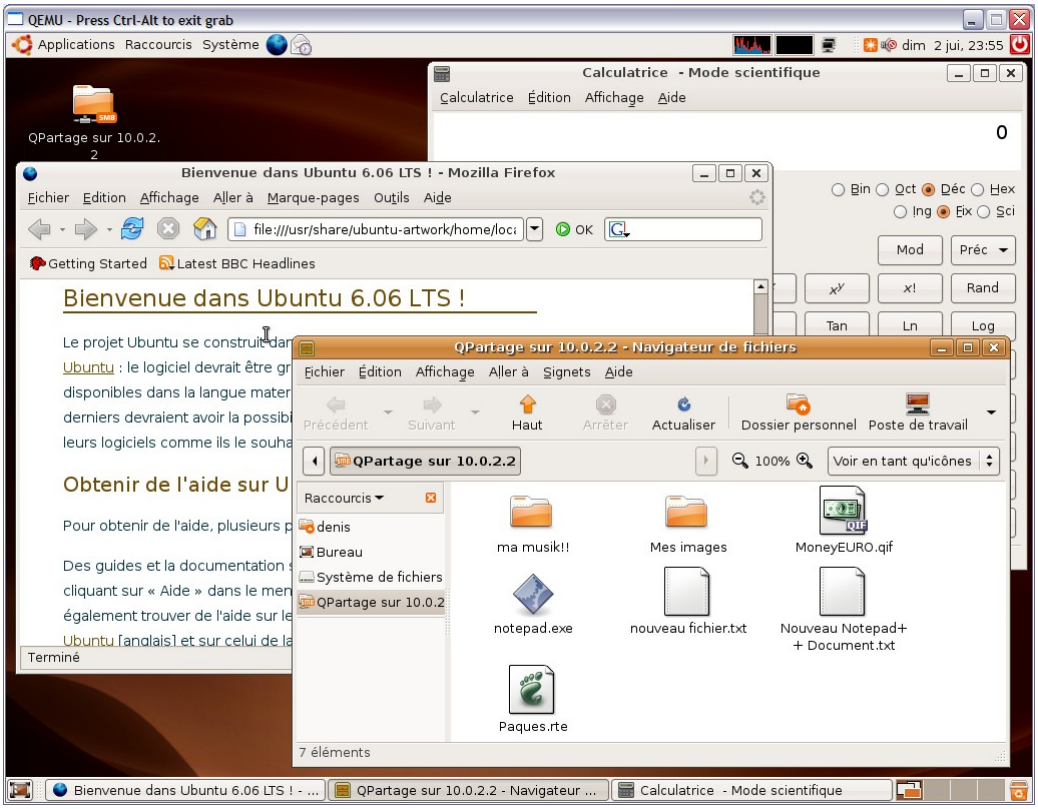


Illustration 7: Ubuntu 6.06 Dapper Drake

Illustration 8: ReactOS 0.3.0 (http://www.reactos.org)

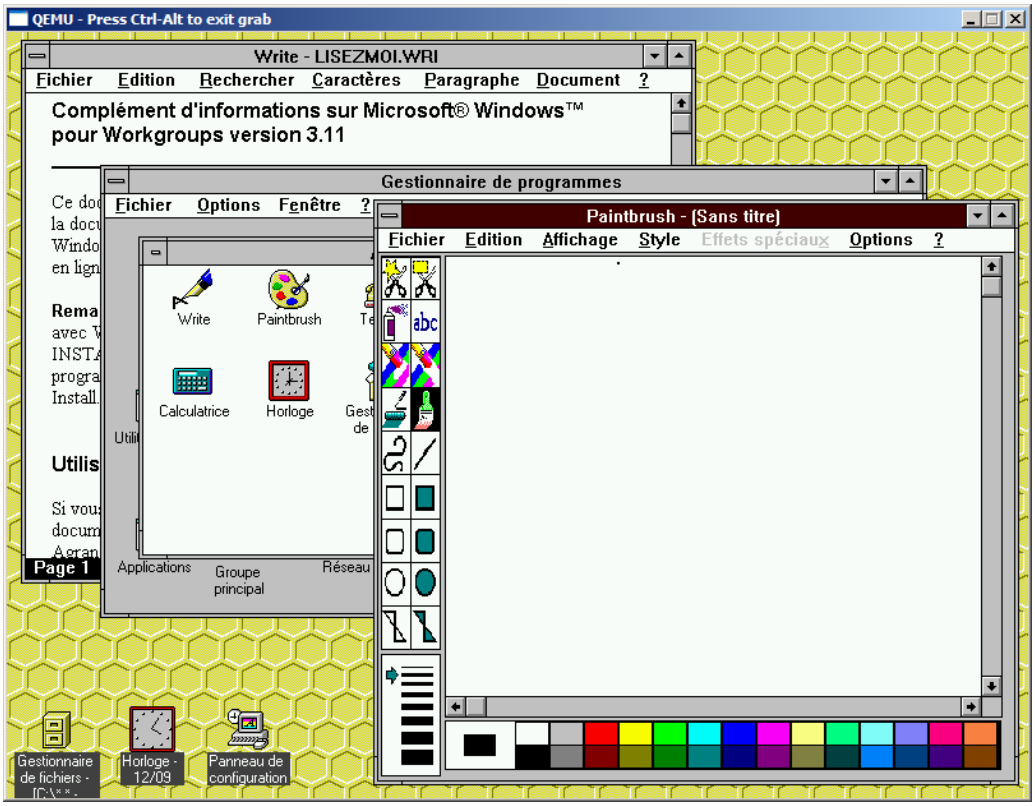


Illustration 9: Nostalgie... Windows 3.11

9 Annexes

9.1 Liste des codes sendkey

HEXA	Touche
0x56	"<"
0x0b	"0"
0x02	"1"
0x03	"2"
0x04	"3"
0x05	"4"
0x06	"5"
0x07	"6"
0x08	"7"
0x09	"8"
0x0a	"9"
0x1e	"a"
0xb8	"alt_r"
0x38	"alt"
0x30	"b"
0x0e	"backspace"
0x2e	"c"
0x3a	"caps_lock"
0x9d	"ctrl_r"
0x1d	"ctrl"
0x20	"d"
0xd3	"delete"
0xd0	"down"
0x12	"e"
0xcf	"end"
0x0d	"equal"
0x01	"esc"
0x21	"f"
0x3b	"f1"
0x44	"f10"
0x57	"f11"
0x58	"f12"

HEXA	Touche
0x3c	"f2"
0x3d	"f3"
0x3e	"f4"
0x3f	"f5"
0x40	"f6"
0x41	"f7"
0x42	"f8"
0x43	"f9"
0x22	"g"
0x23	"h"
0xc7	"home"
0x17	"i"
0xd2	"insert"
0x24	"j"
0x25	"k"
0x52	"kp_0"
0x4f	"kp_1"
0x50	"kp_2"
0x51	"kp_3"
0x4b	"kp_4"
0x4c	"kp_5"
0x4d	"kp_6"
0x47	"kp_7"
0x48	"kp_8"
0x49	"kp_9"
0x4e	"kp_add"
0x53	"kp_decimal"
0xb5	"kp_divide"
0x9c	"kp_enter"
0x37	"kp_multiply"
0x4a	"kp_substract"
0x26	"l"

HEXA	Touche
0xcb	"left"
0x32	"m"
0xdd	"menu"
0x0c	"minus"
0x31	"n"
0x45	"num_lock"
0x18	"o"
0x19	"p"
0xd1	"pgdn"
0xc9	"pgup"
0xb7	"print"
0x10	"q"
0x13	"r"
0x1c	"ret"
0xcd	"right"
0x1f	"s"
0x46	"scroll_lock"
0x36	"shift_r"
0x2a	"shift"
0x39	"spc"
0x14	"t"
0x0f	"tab"
0x16	"u"
0xc8	"up"
0x2f	"v"
0x11	"w"
0x2d	"x"
0x15	"y"
0x2c	"z"

Ce tableau donne la liste des codes de touches acceptés par la commande `sendkey` du moniteur. Il est possible de fournir le code hexadécimal ou le nom de la touche.

10 A faire

- Compléter le chapitre « Architecture réseau de QEmu », notamment les paragraphes concernant le mode TUN/TAP, ainsi que le VLAN, dès que cette option sera prise en charge correctement sous Windows ;
- Description du support des périphériques USB hôte, dès qu'il sera opérationnel sous Windows ;
- Description de l'utilisation des ports série et parallèle de QEmu ;
-

11 Historique des modifications

Juillet 2006 – **Version 1.00** – version initiale.

06/08/2006 – **Version 1.01** – Corrections typographiques. Précisions sur les commandes `commit` et `convert` de qemu-img. Option `macaddr` de la commande `net nic` (5.2.1). Précisions sur le transfert TFTP. Lien vers le site Bochs.

13/09/2006 – **Version 1.02** – Révision du chapitre 2 : ajout du paragraphe « Appliquer un patch. » - Paragraphe 3.3 : mention de qvm86, précisions sur l'accélération par défaut. - Paragraphe 5.1.1.2 : Format qcow2. - Paragraphe 5.2.1.3 : option `-redir`. - Paragraphe 5.2.5 : redirection et VNC. - Paragraphe 5.2.6 : option `-k`. Paragraphe 5.3.5 : options USB. - 5.3.7 : instantanés multiples.

22/01/2007 - **Version 1.03** – Ajout des options `-no-quit`, `-no-reboot`, `-option-rom`.

License pour Documents Libres

Version 1.1

Copyright (©) 2001 Guilde des Doctorants.

Voici le texte de la Licence pour Documents Libres proposée par la Guilde des Doctorants. Ce document est disponible sous forme transparente en LateX et HTML, et sous forme opaque en Postscript et PDF. La source est contituée par le fichier LateX.

---

1 Introduction

Le but de cette licence, rédigée par la Guilde des Doctorants, est de rendre libres les documents écrits auxquels elle s'applique. Un document est dit libre au sens où chacun peut le recopier et le distribuer, avec ou sans modification par tous moyens possibles et imaginables. Cette licence préserve la propriété intellectuelle de l'auteur et de l'éditeur du document. Elle est aussi conçue pour éviter toute récupération commerciale d'un travail bénévole sans le consentement express de ses auteurs. D'autres licences rendant libres des documents, des contenus, des publications existent comme la Free Documentation Licence de la Free Software Foundation et l'initiative OpenContent. Elles sont rédigées en langue anglaise et font parfois référence à des notions de droit américain (notion de fair use). Nous avons très largement repris certains des points de ces licences et nous en avons laissé certains de coté. Néanmoins ces licences comme la LDL partagent une même vocation. La Licence pour Documents Libres (LDL), rédigée en français est sujette à améliorations qui sont les bienvenues (voir section 7).

Cette licence a été conçue pour s'appliquer à divers types de documents quel que soit leur support : documents techniques, notes de cours, documentation logicielle ou encore uvres de fictions. Elle inclut également un "copyleft" pour reprendre la terminologie du GNU : tous les documents dérivés du document original héritent de cette licence.

2 Définitions et domaine d'application

Cette licence s'applique à tout document, quelle que soit sa forme, comprenant la notice standard associée à cette licence. La "notification de licence" désigne la section du texte où sont mentionnés le fait que le document est soumis à la présente licence ainsi que le copyright du document. Un document est produit par un ou plusieurs auteurs. Un document peut être constitué de plusieurs contributions mises en commun. Dans ce cas, l'éditeur désigne la personne morale ou physique qui assure la mise à disposition du document sous diverses formes. S'il n'y a qu'un auteur, il est son propre éditeur. Conformément au code de la propriété intellectuelle, chaque auteur conserve la propriété intellectuelle sur sa contribution. Toutefois, l'éditeur a toute liberté pour faire évoluer le document dans le respect des dispositions de la présente licence. La notice de copyright mentionne l'éditeur si il existe ainsi que les noms des auteurs.

On appellera "version dérivée" tout document comprenant le document de départ partiellement ou dans son intégralité. Une traduction est aussi considérée comme une version dérivée.

La "section historique" du document désigne une partie du document comprenant un historique de sa genèse et de son évolution. Dans le cas d'un document derivé, la section historique contient le descriptif du ou des documents originaux et des modifications qui y ont été apportées. Elle peut également contenir des éléments non factuels comme des considérations éthiques ou politiques concernant l'historique et les motivations du document. La section historique peut donc n'avoir aucun rapport avec l'objet principal du document.

La "Page de titre" désigne pour un document imprimé la page de titre au sens usuel plus les pages de couverture. Dans le cas de documents pour lesquels ces notions ne s'appliquent pas, c'est le texte proche de l'endroit où apparaît le titre du document et la fin du document. La notification de licence sera placée dans la page de titre. La notice standard minimale aura la forme suivante :

"Copyright (c) ANNEE, EDITEUR et AUTEURS. Le contenu de ce document peut être redistribué sous les conditions énoncées dans la Licence pour Documents Libres version x.y ou utlérieure."
Un document peut contenir des "sections invariantes". La liste des titres de sections invariantes est précisée dans la notice spécifiant que le document est soumis à la présente licence. Par exemple :
"Le présent document contient un certain nombre de sections invariantes qui devront figurer sans modification dans toutes les modifications qui seront apportées au document. Leur titres sont: TITRES DES SECTIONS INVARIANTES".
Nous distinguons trois modes de diffusion de documents électroniques: une forme "transparente", ce qui désigne tout format électronique dont les spécifications sont disponibles dans le domaine public ou qui peut être édité par des programmes éventuellement commerciaux largement disponibles à la date de publication du document.

Exemples: ASCII, Texinfo, TeX et LaTeX, RTF, HTML, XML, SGML avec une DTD publique.

une forme "opaque", ce qui désigne tout format électronique permettant l'affichage ou l'impression du document de manière simple au moyen de logiciels du domaine public ou du moins très largement disponibles à la date de publication du document. Un tel format ne permet pas la modification dudit document de manière simple.

Exemples: Postscript, PDF, tout format de traitement de texte nécessitant un logiciel propriétaire, ou tout déclinaison de SGML dont la DTD n'est pas publique.

une forme "cryptée" ce qui désigne le cas où une partie (ou la totalité) du document est sous un format électronique qui n'est pas lisible sans la possession d'une clef logicielle ou matérielle qui en permet le décodage. La forme cryptée peut être utilisée à des fins d'authentification. Une fois décodé le document peut être sous une forme transparente ou opaque. Dans le cas d'une forme cryptée, si l'éditeur n'est plus en mesure de fournir la clef de décodage, il doit rendre disponible le document sous une forme transparente ou opaque non cryptée.

3 Conditions communes aux versions modifiées et intégrales

La distribution de versions intégrales et modifiées du présent document sous n'importe quelle forme est autorisée aux conditions suivantes :
Les notices de copyright spécifiant que le document est soumis à la présente licence ainsi que les sections invariantes doivent être préservées.
Les sections invariantes ne peuvent être altérées.
Les sections historiques ne peuvent être que complétées.
La localisation du document original doit être mentionnée dans la page de titre et de manière visible.
Un document disponible sous forme transparente ne peut être rediffusé sous forme opaque seulement.
Vous ne devez mettre en place aucun dispositif visant à restreindre l'accès au document ou la possibilité de reproduire les copies que vous distribuez. En particulier vous ne pouvez rendre disponible tout ou partie du document sous forme cryptée si l'auteur l'a expressément interdit.
La redistribution dans un cadre commercial ne peut être effectuée sans l'accord préalable des auteurs et de l'éditeur du document original.
Si la distribution de copies du document entraîne des frais de reproduction (photocopies, impressions, pressage de médias), vous pouvez néanmoins

les imputer au lecteur. Mais vous ne pouvez pas percevoir de droits d'exploitation liés au contenu, ni à l'utilisation du document.
Si vous effectuez une diffusion en nombre du document (diffusion sur le WEB, par FTP, ou à plus de 99 exemplaires imprimés, par courrier électronique, sur CDROM, ou sur d'autres supports magnétiques ou optiques), vous devez inclure une copie de la présente licence. Dans ce cas, vous devez également prévenir les éditeurs du document original afin de définir avec eux comment veiller à la diffusion de versions à jour du document.

4 Modifications

4.1 Dispositions générales

Vous pouvez utiliser une partie du présent document, en la modifiant éventuellement, pour produire un nouveau document. Les dispositions de la section 3 s'appliquent.

Vous devez en plus :

lister un ou plusieurs auteurs ou entités responsables des modifications apportées au document.
mentionner sur la page de titre que le document dérivé est une modification d'un ou plusieurs documents originaux. Vous devez préciser leurs titres ainsi que l'entité éditrice ou les principaux auteurs.
préciser sur la page de titre que vous êtes l'éditeur de la version dérivée.
Vous ne devez en aucun cas :
altérer une mention d'un nom d'auteur présent dans le document original et concernant une partie que vous avez réutilisé.
donner au document dérivé le même titre que le document original sans autorisation de l'éditeur de celui-ci.
Nous recommandons de plus que les titres de sections ne soient altérés qu'en cas de changement du plan du document rendues nécessaire par les modifications apportées.

4.2 Fusion ou combinaisons de documents

Dans le cas où le document que vous produisez est issu de la combinaison de plusieurs documents (après modifications éventuelles) soumis eux aussi à la présente licence, vous pouvez remplacer les diverses notifications de licence par une seule.

De même, vous pouvez regrouper les diverses sections historiques pour n'en faire qu'une seule. Elle doit mentionner explicitement les documents originaux auxquels vous avez fait appel et indiquer leur localisation.

Si un des documents utilisé est disponible sous une forme transparente alors la totalité du document dérivé doit aussi l'être.

Vous devez respecter les points listés en sections 3 et 4.1.

4.3 Inclusion dans d'autres travaux

Si le Document ou une de ses versions dérivées est agrégé avec des travaux indépendants, de sorte que plus de 50 % du document final ainsi produit ne soit pas soumis à la présente licence, le document final n'est pas considéré comme une version dérivée soumise dans son ensemble à la présente licence. Néanmoins, la ou les portions du document final qui sont issues d'un document soumis à la présente licence restent soumis à cette licence. Les recommandations des sections 3 et 4 s'appliquent.

4.4 Traduction

Une traduction d'un document est considérée comme une version dérivée. Dans ce cas, vous pouvez néanmoins traduire les sections invariantes. Si vous ne laissez pas les versions originales de ces sections, vous devez prendre contact avec l'éditeur de la version originale afin d'obtenir son accord pour les traductions de ces sections.

La Guilde proposera un certain nombre de traductions de cette licence. Si il en existe une pour la langue cible de la traduction du document, c'est celle-ci qui s'applique. Dans le cas contraire vous êtes invité à proposer une traduction de la licence à la Guilde. Si vous ne le faites pas, ou si la Guilde refuse cette traduction, c'est la version originale qui s'applique.

5 Dispositions concernant la garantie

Cette licence ne définit que les droits de reproduction modification et diffusion du document. Elle n'y associe aucune garantie : sauf mention expresse du contraire, qui n'engagerait alors que l'éditeur du document, et dans la mesure où le contenu est en conformité avec la législation française, il est entendu que ni l'éditeur ni les auteurs du document ne sauraient être tenus pour responsables des éventuels dommages et préjudices que l'utilisation du document aurait entraîné. Ces dispositions s'appliquent même s'il s'avère que le document contient naturellement ou par obsolescence une inexactitude, une imprécision ou une ambiguïté.

Tout auteur ou éditeur souhaitant doter un document soumis à la présente licence de dispositions de garantie doit joindre à chaque copie distribuée du document un certificat de garantie précisant exactement les dispositions de garantie et mentionnant explicitement les noms des personnes morales ou physique assumant les responsabilités de la garantie. Les dispositions de libre copie de la présente licence restent valable pour un document avec garantie mais toute rediffusion par une autre personne que l'auteur du certificat de garantie se fait sans garantie.

6 Cessation de la licence

Vous ne pouvez redistribuer le présent document ou une de ses versions dérivées sous une licence différente. Cela entraînerait l'annulation des droits de copie, modification et distribution du document.

En soumettant un document à la présente licence, vous conservez les droits de propriété intellectuelle liés à votre qualité d'auteur et vous acceptez que les droits de reproduction, diffusion et modification du document soient régis par la présente licence.

7 Évolution de la licence

La Guilde des Doctorants se réserve le droit de faire évoluer la présente licence. Elle s'assurera de la compatibilité ascendante des différentes versions. Chaque version de la licence est numérotée.

Sauf mention explicite, il est sous entendu que si le document précise un numéro de licence, cela signifie que toute version ultérieure convient. Si aucun numéro n'est précisé, cela signifie que toute version de la licence convient.

La présente licence s'applique à elle-même. Vous pouvez donc la modifier, à condition d'en changer le titre et de préserver comme section historique l'introduction. Vous devez également préserver le plan du présent document.